پاراستنی زانیاری

Information Security

م.هێمن مەلا کەریم بەرزنجی

بەکالۆریۆس و ماستەر ی کۆمپیوتەر

زانکۆی پۆلیتەکنیکی سلێمانی

کۆلێژی ئینفۆرماتیك – بەشی ئای تی

پەیمانگەی زانستی کۆمپیوتەر – بەشی ئای تی

ناوی کتێب : پاراستنی ((ئاسایشی)) زانیاری Information Security.

نوسینی : هێمن مەلا کەریم بەرزنجی

پیتچنین و نەخشەسازی ناوەوە : هێمن کەریم ئەحمەد

تیراژ : ٣٠٠٠ دانە

نۆبەتی چاپ : یەکەم ٢٠١٢، دووەم ٢٠١٦

ساڵی چاپ : ٢٠١٦

Mobile: 07701515582

E-Mail: hemnbarznji82@gmail.com

dr.hemn@yahoo.com

Personal Website(Weblog):

www.hemnbarznji.blogspot.com

Facebook:

facebook.com/hemn.melakarimbarznji

پاراستنی

زانیاری

Information

Security

نووسینی:هێمن مەلا کەریم بەرزنجی

ماستەر لە زانستی کۆمپیوتەر

زانکۆی پۆلی تەکنیکی سلێمانی

کۆلێژی ئینفۆرماتیك و پەیمانگەی زانستی کۆمپیوتەری سلێمانی

چاپـــــی دووەم

٢٠١٦

پێشکەشە بە:-

- **رۆحی پاکی مەرحومی باوکم ((حاجی بابا شێخی بەرزنجی)) رەزا و رەحمەتی خوای لێبێت، یەکەم مامۆستا و ڕێبەری ژیانم.**
- **دایکم و هەردوو براکەم.**
- **هەموو ئەو مرۆڤانەی بێوچان و بەردەوام لە هەوڵی فێربوون و، بەخشینی زانستدان.**
- **هەموو ئەو مامۆستایانەی لە حوجرەو قوتابخانەکانەوە، تا ئەمڕۆ، تەنها وشەیەك چییە لێیانەوە فێر بووبم.**
- **ئەو مرۆڤەی دەبێتە بە شێك لە ژیانم و خۆشم دەوێ و خۆشی دەوێم. ئەگەرچی نازانم کێ یە و، چۆن و، کەی ؟!!**

پێشەکی :

ئاسایشی زانیاری یان پاراستنی زانیاری یەکێك لە گرنگترین بوارەکانی تەکنەلۆژیایە و، ناکرێت و ناگونجێت بمانەوێت سیستەمی ئەلیکترۆنی و تەکنەلۆژی درووست بکەین، بێ ئەوەی گرنگی بە بواری پاراستن بدەین. چونکە لە دونیای تەکنەلۆژی دا زیاتر زانیاری رووبەرووی مەترسی و فەوتان و کەوتنە دەست ناحەز و خراپەکار دەبێتەوە، وەك لە دوونیای کۆن و کاغەز و ئەرشیفی مادی گەورەی فایل و مامەڵە و زانیاری سەر کاغەز.

بۆیە بە پێویستم زانی کتێبیکی تایبەت بە بووارى ((پاراستنی زانیاری)) بنووسم و، تاراوەکیش و بە گوێرەی توانا هەولبدەم گرنگی بە بووارى کرداریش بدەم و ، نموونەی لە بارەوە بهینمەوە، بۆ ئەوەی فێر خواز وەرس نەبێت لە خویندنەوەی کتیبەکە و، بەکارهێنانی، هەروەها بە ئاسانتر لە مانا و مەبەستی بابەتەکان تێبگات.

جیگەی ئاماژەیە کە بەرهەمەکە ئەکادیمییە و بە پشت بەستن بە چەندین سەرچاوەی جیهانی و نیودەوڵەتی نووسراوە و، هەولیش دراوە وشە و زاراوەکان بە کوردی بکرێت و، بە ئینگلیزیش وەك خۆی بنووسرێتەوە، بۆئەوەی بەکاربەری ئەم کتیبە هەم وشە ئینگلیزییەکە بزانێت بۆ ئەوەی کە کتیبێکی ئینگلیزی بووارەکە دەخوێنێتەوە بە باشتر لێی تێبگات، هەروەها ماناکەشی بە زمانی کوردی نووسراوە و، ئەگەر پێویستی بە راڤە بووبێت ئەوا شیمان کردۆتەوە.

لە کۆتایدا هیوادارم توانیبێتم خزمەتێك بە بواری زانستی کۆمپیوتەر و تەکنەلۆژیایی زانیاری بکەم و، کەم تازۆر ڕۆڵمان هەبووبێت لەبەرەو پێشبردنی کۆمەڵگەی کوردی دا، وەلێ نابێت ئەوەش لەیادبکەین کە ئەم بەرهەمە ئەنجامی شەونخونی و هەولێ و ماندوبونێکی زۆرەو لەگەڵ ئەوەشدا بێکەم و کوڕی نییە

هێمن مەلا کەریم بەرزنجی

کوردستان – سلێمانی

٢٠١٥/٣/٢٥

بەشی یەکەم

ناساندنی پاراستنی زانیاری

Introduction to Information Security

زانیاری Information

زانیاری دەتوانرێت پێناسە بکرێت بەوەی کە زانیاری شیکار نەکراو ((داتا Data)) ی وەرگێراوی مانادارە Meaningful Translated Data، ئەگەر ئێمە ژمارەیەکمان هەبێت82-55-151 ناتوانین هیچ رستەیەك درووستبکەین لە سەر خاوەنەکەی، ئەوە تەنها زانیاری شیکار نەکراوە ((داتا – Data)) ، بەلام کاتێك دەڵێین، ژمارەی مۆبایل : ۰۷۷۰۱۵۱۵۵۸۲، ئیدی رستەیەك دەستپێدەکات، ئەویش ژمارەی مۆبایلە ،ئەمانەی خوارەوەش نموونەی ترن:

ناونیشان: هەرێمی کوردستان – شاری سلێمانی.

گەرەك: رۆژهەڵات، گەرەك:۳۰۹، کۆلان:٦۰.

ئەمە زانیارییەکی زۆر بەسوودە، ناونیشانی نووسەری ئەم کتیبەی بەردەستە و، تیایدا شوێنی نیشتە جێبوونی دیاری کراوە.

هەربۆیە لە رووانگەی شیکەرەوەی سیستەمەوە System Analyst، زانیاری بریتییە لە زنجیرەیەك هێما کە دەتوانرێت بەکاربهێنرێت بۆ درووستکردنی نامە و پەیامێکی سوودبەخش.

بەپێی پێناسەی ویکی پێدیا، زانیاری :

زانیاری یەکان دەتوانرێت تۆماربکرێت وەکو نیشانەکان Signs، یان بگوێزێتەوە وەکو هێماکان ((سیگناڵ – Signals))، زانیاری هەر جۆرێکی رووداوە کە کاریگەری هەبێت لەسەر دۆخی جولاوی سیستەم کە دەتوانرێت زانیارییەکە وەربگێردرێت.

بەلام بە گوێرەی پێناسەی داڤیس و ئۆسلۆن Davis and Oslon:

زانیاری Information داتایە Data کە چارەسەر کراوە و گۆردراوە بۆ شێوەیەك کە مانا بەخش و مەبەست داربێت، بۆ ئەوەی وەربگیرێت، یان راستەقینەیەکە، یاخود نرخێکی هەستپێکراوە لە ئیستا دا، هەروەها دەگونجێت گرینمانەی رووداوێك بێت، یان بریاری وەرگرتنێك.

جیاوازی نێوان داتا و زانیاریData & information

داتا چییە؟

What is Data?

داتا دەتوانرێت پێناسەبکرێت وەکو پیشاندانی راستی یەکان Facts، چەمك و بیرۆکەکان Concepts یان رێنمایی و زانیارییەکان Instruction لە شێوازی رەسمی کردنی شتەکان دا، کە گوونجاوە بۆ گەیاندن و پەیوەندی، تەفسیر و راڤە Interpretation یان چارەسەرکردنی لەلایەن مرۆڤەوە Human یان ئامێری ئەلکترۆنی Electronic Machine. یان دەتوانین بلێین گرووپێکە لە هێماکان Groups of Symbols کە عەشوائی نییە Non – Random، لە شێوەی نووسین ((دەق)) Text، وینە Image، دەنگ Voice، کار Action و تەنەکان Objects.

داتا پیشاندەدرێت بە یارمەتی کارەکتەرەکان Character وەکو ئەلف و بێ A,B,C –a,b,c، ژمارە(۰-۹) digit، یان کارەکتەری تایبەتی وەکو (+،-،/،*،=، .....)).

زانیاری چییە؟

What is Information?

زانیاری داتای ڕێکخراوە Organizedیان پۆلێنکراوە Classified ، کە نرخێکی مانا بەخشی هەیە بۆ بەکارهێنەر و وەرگر Receiver. زانیاری داتای چارەسەر کراوە کە بریاردانەکان و، کردارەکان بنچینەن.

بۆ بریاردانی مانابەخش و مانادار Meaningful پێویستە زانیاری چارەسەر کراو موئەهەل بێت، بۆ ئەم ڕووخسار و تایبەتمەندییانەی لای خوارەوە:

١. گونجاو، هاوکات ئامادەبێ Timely: پێویستە زانیارییەکە ئامادەبێت کاتێك پێویست بوو و داواکرا.

٢. دیقە Accuracy:پێویستە زانیارییەکە ورد و بە دیقەت بێت.

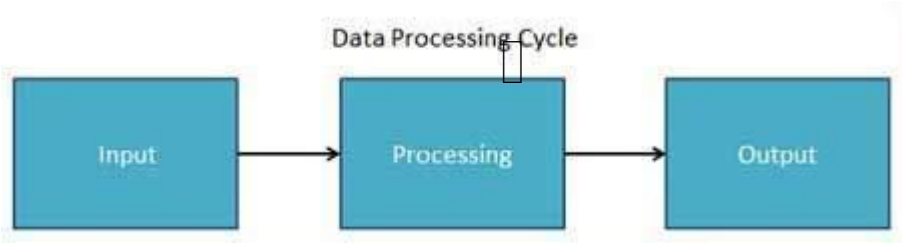
٣. تەواوێتی Completeness: پێویستە زانیارییەکە تەواو بێت.

سووری چارەسەر کردنی زانیاری شیکارنەکراو

Data Processing Cycle

چارەسەرکردنی داتا، بنیاتنانەوە و دڕووستکردنەوە یان ڕێکخستنەوە و ڕێککردنەوەی زانیاری یە لەلایەن خەڵکەوە، یان لەلایەن ئامێرەوە، بۆ زیادکردنی بەسوودی و زیاد کردنی نرخ بۆ مەبەستێکی دیاری کراو و تایبەت.

چارەسەرکردنی داتا پێکدێت لە هەنگاوە بنچینەییەکانی داغڵکردن Input، چارەسەر کردن Processing و بەرهەم Output. ئەم سێ هەنگاوە سووڕی چارەسەر کردنی داتا پێکدەهێنن.



- داغلّکردن Input: لەم هەنگاوەدا داتای داغلّکراو ئامادە دەکرێت لە هەندێك شێوە Form ی گوونجاودا بۆ چارەسەر کردن Processing. شێوەکەش The Form پشت دەبەستێت بە ئامێری چارەسەر کردنەکە، بۆ نموونە، کاتێك کۆمپیوتەرە ئەلیکترۆنیکییەکان بە کار دەهێنین، داتای داغلّکردن دەتوانرێ تۆمار بکرێت لە یەکێك لە جۆرە جیاوازەکانی ناوەند و هۆکاری داغلّکردنەوە، وەکو دیسکی موگناتیسی Magnetic disc، شریتەکان Tapes و هەروەها .
- چارەسەر کردن Processing: لەم هەنگاوەدا زانیاری داغلّکراو دەگۆرێت بۆ زانیاری بەرهەم و دروستکراو Produce data لە شێوە Form ی بەسوود دا، بۆنموونە پارەدان لەوانەیە ئەژمار بکرێت لە رێگەی کارتەکانی کاتەوە، یان پووختەی فرۆشتنی مانگێك لەوانەیە ئەژماربکرێت لە حساباتی فرۆشتنەوە.
- بەرهەم ((وەرگرتنەوە)) Output: ئەمەش ئەنجامی بەرهەمی هەنگاوی چارەسەر کردنە بە کۆکراوەی، شێوەی دیاری کراوی زانیاری ((داتای)) بەرهەم پشت دەبەستێ بە Depend بەکارهێنانی زانیارییەکە، بۆ نموونە داتای بەرهەم لەوانەیە لە پارەدانەوە بێت بۆ فەرمانبەران.

زانیاری، زانست و مەعریفە، و زیرەکی کار و بار

Information, Knowledge & Business Information

پرۆفیسۆر رای ڕ. لارسۆن Ray R. Larson لە سکولّی زانیاری School Of Information لە زانستگەی کالیفۆرنیا University Of California، بێرکیلی Berkeley، هەرەمی زانیاری Information Hierarchy بەم جۆرەی خوارەوە دادەڕێژێت:

١. داتا Data، یان زانیاری شیکار نەکراو ، مادەی خاو The Raw Material ی زانیاری Information یە.
٢. زانیاری Information: داتای رێکخراوە Organized Data، و پیشان دەدرێت لە لایەن هەر کەسێکەوە.
٣. زانست و مەعریفە Knowledge: زانیاری خوێندراوە، بیستراو، یان بینراو و هەستپێکراوە.
٤. حیکمە Wisdom: مەعریفە و زانستی یەکپارچە و بەیەککراوە و پوختەکراوە بۆ تێگەیشتن و بەکارهێنان.

بەڵام سکۆت ئەندریۆ Scott Andrew، بەم جۆرەی لای خوارەوە پۆلێنکاری دەکات و پێناسەکان دەخاتە روو::

١. داتا Data: راستەقینەیەکە Fact یان پارچەیەکە لە زانیاری Piece of Information یان زنجیرەیەکە لەوانە.
٢. زانیاری Information: زانست و مەعریفەی وەرگیراو و دیاری کراوە لە داتاوە.
٣. زیرەکی کار و بار Business Intelligince: بەریوەبردنی زانیاری گرێدراو و پەیوەست بە سیاسەتی رێکخراوە و، بریارەکانی.

پاراستن ((ئاسایشی))
Security

بە شێوەیەکی گشتی، زاراوەی پاراستن Security لە وێبستەر Websterدا، پێناسە کراوە بەوەی کە : ((جۆرێتی یان هەرێمێ پارێزراوبێت The quality or state of being secure، وەکو رزگاربوون لە ترسناکی Freedom from danger، سەلامەتی Safety، رزگاربوون لە ترس و رارایی Freedom from fear or anxiety.

هەروەها لە پێناسەیەکی تردا، دەوترێت: سیستەمێکە یان کۆمەلێك هەنگاوە کە یارمەتی هێشتنەوە و پاراستنی زانیاری دەدات لە کەوتنە بەرچاو و بەردەست کەوتن، لە ماوەی بەکارهێنان یان ناردنی دا. ئەم پاراستنە بە هۆی تێپەرە وشەوە Password بێت، یان بە گۆرینی زانیاری بۆ شێوەیەك کە نەزانرێت چیيە Encryption و هەروەها بە هۆی شاردنەوەوە Hiding، لە کاتێکدا پاراستن Security دڵنیای تەواو و سەد لە سەد نادات بەوەی کە زانیاری دوو چاری ترسناکی و دزین و فەتاندن و تێکدان نەبێتەوە، بەڵام تا ئاست و هەنگاوەکانی پاراستن زیاتر بێت، دڵنیایی پاراستنی زانیاریش لە ترسناکی Danger زیاتر دەبێت.

پاراستنی زانیاری
Information Security

پاراستنی زانیاری Infosec یان Information Security: زاراوەیەکی گشتی یە، کە بەکاردەهێنرێت بۆ وەسفکردنی جیبەجێکردن و کرداری پاراستنی زانیاری لە دەست پێگەیشتنی نەخوازراو Unwanted Access، یاخود جیبەجێکردنی نەخوازراو . کە بەشێوەیەکی تایبەتی جیبەجێدەکرێت لەلایەن سووپاوە، یان حکومەتەوە، یان کۆمپانیا و دامەزراوەکانەوە، بۆ ئەوەی زانیاری ورد و بە بایەخ لە دەست نەدەن و نەکەوێتە

دەست کەس، کە ببێتە هۆی هەڕەشە و ترسناکی مادی و ستراتیجی ئەگەر بکەوێتە بەردەست کەسانی تر جگە لە خاوەنی زانیارییەکە.

بەڵام پێناسەی پاراستنی زانیاری بە گوێرەی ((پێوەرە بلاوکراوەکانی لیژنەی سیستەمی پاراستنی نەتەوەیی standards published by the committee on national security system ((CNSS)) و لیژنەی نیشتیمانی گەیاندنی پاراستن و پاراستنی زانیاری the national security telecommunications and information System security committee ((NSTISSC))))بریتییە لە : پاراستنی زانیاری و دانە گرنگەکانی، سیستەم و ئامێرەکانیش دەگرێتەوە کە بەکاردێت لە، پاشەکەوتکردن، و گواستنەوەی زانیاری.

Information security is the protection of information and its critical elements, including the system and hardware that use, store and transmit that information.

پاراستن Security، لە پیشە سازیی کۆمپیوتەر Computer Industry دا ، زاراوەی پاراستن Security، یان پاراستنی کۆمپیوتەر Computer Security، دەگەڕێتەوە بۆ هەموو ئەو تەکنیك و ڕێگایانەی کە بەکاردێت بۆ دڵنیابوون لە زانیاری Data پاشەکەوتکراو لە کۆمپیوتەر دا، تا نەتوانرێت بخوێنرێتەوە یان بکەوێتە مەترسییەوە لە لایەن کەسی ڕێگە پێنەدراوەوە، زۆربەی پێوەرەکانی پاراستنی کۆمپیوتەر لە شێوەی شیفرەی زانیاری Data Encryption و تێپەڕەوشە Password.

فرە چینی پاراستن
Multiple Layers of Security

ڕێکخراوێکی سەرکەوتوو پێویستە ئەم فرە چینەی خوارەوەی هەبێت لە پاراستن لە شوێنەکەی دا، بۆ پاراستنی کارەکان و شتەکان و زانیارییەکان:

١. پاراستنی مادی Physical Security: بۆ پاراستنی شتە ماددییەکان ((فیزیاییەکان)) ، تەنەکان Objects و ڕووبەڕەکان لە دەستپێگەشتنی ڕێگەپێنەدراو Unauthorized Access و خراپ بەکارهێنان Misuse.
٢. پاراستنی کەسی Personal Security: بۆ پاراستنی خودی ((شەخس)) و کۆمەڵە کەسێك کە ئەوانەن دەسەلاتیان پێدراوە Authorized بۆ دەستگەیشتن بە ڕێکخراوەکە و کارکردن تیاید.

٣. پاراستنی کردارەکان Operations Security: بۆ پاراستنی وردەکاری کرداری تایبەت و زنجیرەیی چالاکی.
٤. پاراستنی گەیاندن Communications Security: بۆ پاراستنی ناوەندی گەیاندن Communications Media، تەکنەلۆژیا Technology و ناوەرۆك Content.
٥. پاراستنی رایەڵە Network Security: بۆ پاراستنی بەشە پێکهێنەرەکانی رایەڵە Network Component، پێکەوەبەستنەکان Connections و ناوەرۆك Content.
٦. پاراستنی زانیاری Information Security: بۆ پاراستنی پێداویستی و دارایی.

تایبەتمەندییە گرنگەکانی زانیاری
Critical Characteristics of Information

هەرچی نرخی زانیارییە وەردەگیرێت لە تایبەتمەندی و رووخسارە زانروەکانی خۆیەوە، کاتێك کە تایبەتمەندی زانیاری دەگۆڕێت، نرخی زانیاریش یان زیاد دەکات Increase، یان وەك زۆر باوە کەم دەکات Decrease، هەندێك لە تایبەتمەندییەکان کاردەکەنەسەر نرخی زانیاری بۆ بەکارهێنەری زیاتر لەوانی تر. ئەمەش پشت دەبەستێت بە بارودۆخەکان، بۆ نموونە: کاتی دیاری کراوی زانیاری کە گونجاوە ببێت بە فاکتەرێکی گرنگ. لەبەرئەوە زانیاری زۆر وونەبێت و دەفەوتێت یان درەنگ دەگوێزرێتەوە.

بەئاسانی دەست کەوتن ((بەردەست))Availability

زانیارییەکە ئامادە و بەردەستە لەکاتێکدا بەکارهێنەری رێگەپێدراو Authorized User داوای دەکات، کەواتە بەردەستبوون ((بەئاسانی دەست پێگەیشتن Availability)) رێگەپێدانی بەکارهێنەرە دەسەڵات پێدراوەکانە، یانە کەسە Persons ریگە پێدراوەکانە، یان سیستەمی کۆمپیوتەر Computer System ، بۆ دەستگەیشتن بە زانیاری Access Information بە بێ ئەوەی هیچ دەستێوەردان Interference و کۆسپخستەرێیەك ((دوواخستن)) Obstruction رووبات، هەروەها بۆ وەرگرتنی ئەو زانیارییە Receive بە شێوەی Format داوا کراو.

تەواوی و بێهەڵەیی Accuracy

زانیاری تەواو و راستە، لە کاتێکدا زانیارییەکە هەڵەکان و بەهەڵەتیگەیشتن Mistake or error تیانەبێت. هەروەها زانیاییەکە نرخیکی هەیە کە بەکارهێنەر چاوەروانی ئەکات. ئەگەر زانیارییەکە بە ئەنقەست یان بەبێ ئەنقەست دەستکاری بکرێت و گۆڕانکاری بچووکی تیابکرێت Change and Modify، ئەوا

زانیارییەکە تەواو و بێهەڵە نابێت.

ساغکردنەوە ((مۆر کردن)) Authentication

ساغکردنەوە((مۆرکردن)) ی زانیاری جۆر یان حاڵەتی پێکهێنەری راستەقینە و ئەسڵییە، زیاتر لەوەی کە درووستکراو یان هەڵبەستراوبێت. زانیاری ساغدەکرێتەوە کاتێك زانیاری بییەکە لەهەمان دۆخ دا بێت کە زانیارییەکە درووستکراوە بۆیی Created ، دانراوە Placed، پاشەکەوت کراوە Stored، یان گواستراوەتەوە بۆیی Transferred.

پرۆسەی دیاری کردنە، کە بەکارهێنەرێك ((کور/کچ)) رایدەگەیەنێت رێگە پێدراوە و خاوەنی ئەژمارە، بۆ ئەوەی ساغ ببێتەوە ئایا راگەیاندنەکەی راستە یان نا؟ بەشێوەیەکی گشتی ناوی بەکارهێنەر User Name و تێپەڕە وشە Password باوترین شێوەی ساغ کردنەوەیە کە ئەمرۆ بەکاردەهێنرێت، بۆ دەستگەیشتن Access بە کۆمپیوتەر و زانیاری، ناسینەوەی زیندەزانی ژمێرەیش Biometric Identification دەتوانرێت بەکاربهێنرێت بە هۆی بەراورد کردنی زانیاری تۆمارەکانی بنکەی زانیاری Database Record بۆ دڵنیابوون و ساغکردنەوەی ئەو بەکارهێنەرەی رای دەگەیەنێت کەسی رێگە پێدراو و خاوەنە.

دەسەلاتنامە ((رێگەپێدان)) Authorization

رێگەدان بە دەستپێگەیشتنی سەرچاوەکان Resources، بە گوێرەی ئەو سنوور و دەسەلاتەی پێی دراوە. رێگەپێدان کرداری دڵنیاکردنەوەیە و، بەهۆیەوە سنووری کار کردنی دیاری دەکرێت، بۆ جیبەجێکردنی کارێکی دیاری کراو، ساغکردنەوە پێویستە پێش رێگەپێدان و دەسەڵات پێدان بێت.

دیاری کردن ((ناسینەوە)) Identification

دان نانە ((ئیعتراف)) بە کەسەکان دا، بۆ ئەوەی هەلبستن بە جیبەجێکردنی کارێکی دیاری کراو، لە وانەیە ناسینەوە لە رێگەی ناوی بەکارهێنەر User Name و تێپەرە وشە Password بێت ، بۆ بەکارهێنانی کۆمپیوتەر، نموونەیەکی تر وەك مۆلەتی شۆفێری، پاسپۆرت، ئای دی کارتی نیشتمانی، بەکارهێنانی ناسنامەی زیندەزانی ژمێرەیی Biometric بەزۆری پشت دەبەستێت بە شوینکەوتنی خێرای ئای دی، وەکو پەنجە مۆر Finger Print، و ..... .

جۆرەکانی ساغکردنەوە

Types of Authentication

سێ ڕێگەی جیاوازمان هەیە بۆ ساغکردنەوە، کە پێویستە زانیاری لە بارەوە بخەینە ڕوو:

١. چی یە ئەو What You Have: لە شێوەی کلیل Key، باج Badge، ئای دی ID، هیماکان Tokens.
٢. چی هەیە ئەو What You Are: پەنجە Finger، لەپی دەست Palm Print، بیلبیلەی چاو Iris pattern.
٣. چی ئەزانێت What Are Know: تیپەڕە وشە Password، دەربڕینی تیپەڕین Passphrase.

نهێنی

Confidentiality

زانیاری باری نهینی و باوەڕپێکراویی Confidentiality هەیە، لەکاتی خستنەڕوو و پیشاندان بۆ کەسی ڕێگەپێنەدراو، یان سیستەمەکان و پاراستنی لێیان، نهێنێتی دڵنیابوونەوەیە لەوەی کە تەنها ئەوانەی مافیان هەیە و ڕێگەیان پێدراوە و لە سنووری ڕەزامەندیدان بتوانن دەستیان بە زانیاری بگات و، بتوانن کاری لەسەر بکەن.

کاتێك کەس یان سیستەمی ڕێگە پێنەدراو، بتوانن زانیارییەکە ببینن، ئەوا نهێنییەکە تێکشاکەوە و، گۆڕاوە. چونکە نهێنی بوون وەك ڕووخسار و تایبەتمەندییەکی زانیاری وایە و، پشت دەبەستێت بە ڕووخسار و تایبەتمەندی تربە زۆری پەیوەندی هەیە بە ڕووخسار و تایبەتمەندی زانراوەوە وەکو تایبەتی Privacy.

کەواتە دەتوانین بە کورتی بڵێین، نهێنی : ئەو زاراوەیەیە کە بەکاردەهێنرێت بۆ وەسف کردنی زانیارییەك کە پارێزراوە لە لە هەر بەکارهێنەرێکی تر کە پێویستە دەستی پێی نەگات. چونکە ڕێگەی پێنەدراوە لە لایەن خاوەنی زانیاری .

سەلامەتی

Integrity

سەلامەتی زانیاری Data Integrity یان سەلامەتی Integrity، زاراوەیەکە و، بەکاردەهێنرێت بۆ وەسفکردنی زانیاری یان فایلی کۆمپیوتەر ی پارێزراو ی باوەڕپێکراو و پاك و پوخت ، کە نەسراوەتەوە یان نەگۆراوە بە رێگەی هەڵە.

زانیاری Information حاڵەتی سەلامەتی هەیە، کاتێك زانیارییەکە هەمووێەتی Whole، تەواوە Complete، و گەندەڵ نەبووە Uncorrupted. سەلامەتی زانیاری دەکەوێتە ژێر هەڕەشەوە Threatened، کاتێك زانیارییەکە زانرابێت و پیشابدرێت بۆ گەندەڵ بوون Corruption، وێرانبوون Damage، تێکشکان Destruction، یان هەر وەستاندن و لەکارخستنێك.

گەندەلیش Corruption لەکاتێکدا رووەدات کە زانیارییەکان دەست بە پاشەکەوت کردن Storeدەکەن، یان دەگوێزرێنەوەTransmitted ، هەندێك لە ڤایرۆسەکانی کۆمپیوتەر و کرمەکانی کۆمپیوتەر بۆ مەبەستی گەندەلکردنی زانیاری بەکاردەهێنرێن.بەلام گەندەلبوونی فایلەکان تەنها بەهۆی هێزیی دەرەکییەوە نی یە، وەکو چەتە Hackers، بەڵکو لەوانەیە بەهۆی دروستبوونی گرفتەوە بێت لەکاتی گواستنەوەدا، یان هەر هۆکارێکی تر.

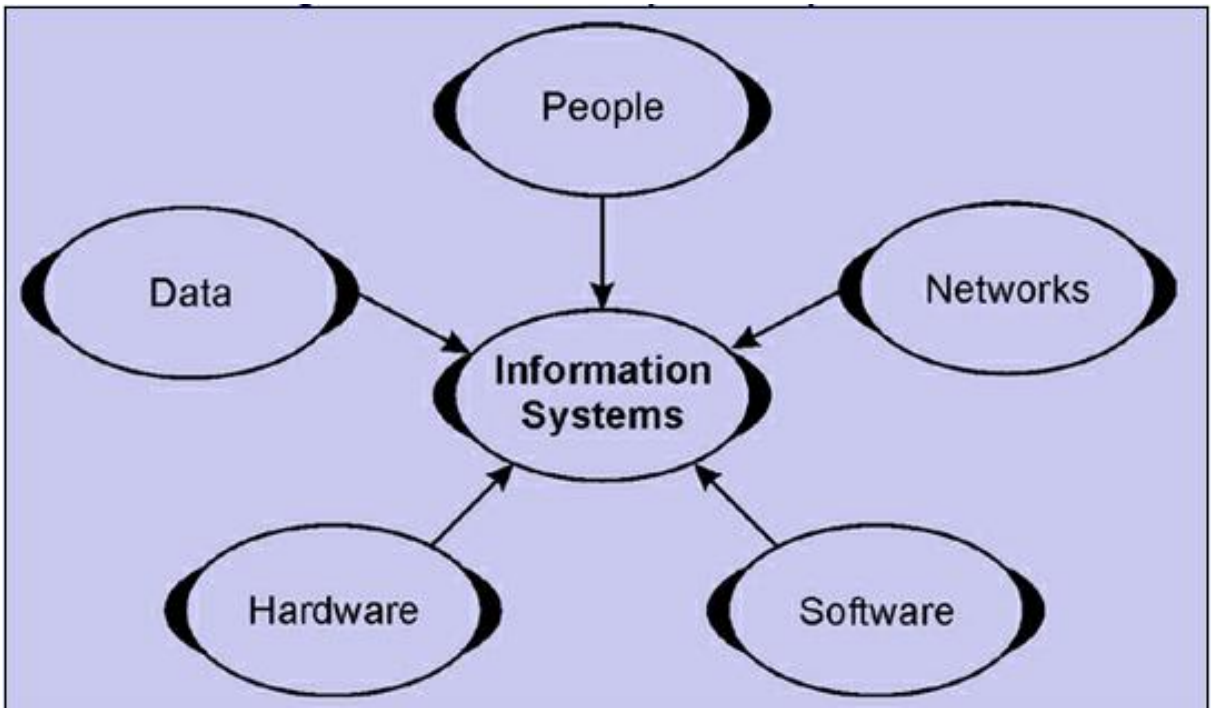
بەشە پێکهێنەرەکانی سیستەمی زانیاری

Components of Information System (IS)

سیستەمی زانیاری Information System، سیستەمێکە System کە داتا Data کۆدەکاتەوە و، زانیاری بلاودەکاتەوە بۆ یەك مەبەستی دیاری کراو، ئەمەش دابینکردنی زانیاری یە بۆ بەکارهێنەر، یان بەمانایەکی تر و ، لە پێناسەیەکی تر دا، دەتوانین بڵێین:: سیستەمی زانیاری : کۆکراوەی کۆمەڵێك بەشی پێکهێنەری پەیوەندی دارە، کە کۆکردنەوە Collect، پرۆسە Process، پاشەکەوت کردن Store، و دابینکردن Provide و بەرهەم Output لە خۆ دەگرێت.

ئامانجی سەرەکی سیستەمی زانیاری ، دابینکردنی زانیارییە بۆ بەکارهێنەرەکانی،سیستەمی زانیاری جۆراو جۆرن و، بەگوێرەی جۆری بەکارهێنەرەکانە کە چی سیستەمیك بەکاردەهینن.

کەواتە سیستەمی زانیاری Information System (IS) بەتەنها ئامێرەکان و پارچەرەقەکان Hardware نی یە، بەڵکو کۆمەڵێکی تەواوە لە ((بەرنامە Software، پارچەرەقەکان/ئامێرەکان Hardware، زانیاری شیکارنەکراو Data، خەڵك People، شێوە و پەیرەوی جیبەجێکردن Procedures، رایەڵە پێوێستەکان Necessary Networks بۆ بەکارهێنانی زانیاری وەکو سەرچاوە لە رێکخراوەکە Organizationدا. ئەم شەش پێوەرە و بەشە پێکهێنەرە بەکاردێن بۆ داغڵکردن Input، چارەسەر کردن Processed، بەرهەم Output و پاشەکەوت کردن Store.



یەکەم// بەرنامە Software:

بەرنامەیەکێکە لە بەشی پێکهێنەری سیستەمی زانیاری یە، کە دابەشدەکرێت بۆ دووبەش ئەوانیش بەرنامەکانی نەزم System Software و بەرنامەکانی جیبەجێکردنن، بەڵام بە گوێرەی هەندێك پۆلێن و دابەشکردنی تر، سێ بەشن، ئەوانیش: بەرنامەکانی جێبەجێکردن Applications، سیستەمی کارپێکردن Operating Systemو یوتیلیتی Utility. گرنگترین بەرنامەکانیش بۆ سیستەمی زانیاری، بەرنامەکانی پاراستنی سیستەمی زانیاری یە.

چەمکی بەرنامە – Software Concept

بۆ ماوەیەك کۆمپیوتەر لەبیر بکە و وازی لیبهینە، لە کاتیکدا بیرۆکەیەکت هەیە و دەتەوێت بە لاپەرەیەکدا بێیتە خوارەوە و لەسەری بنووست، ئەگەر ویستت سەرنجی زبر و ناڕێك و پێچاو پێچ بنووسیت، ئەوا ئەگەری ئەوە هەیە قەڵەم هەلبژێریت، ئەگەر بتەوێت نامەیەك بنووسیت، ئەوا ئەگەری ئەوە هەیە جاف هەلبژێریت، ئەگەر بتەوێت وێنەکێشی بکەیت، ئەوا ئەگەر ئەوە هەیە فڵچە هەلبژێریت.تۆ باشترین ئامرازت هەلبژارد بۆ کارەکە.

کاتی بەکارهێنانی کۆمپیوتەر، ئامرازەکان چالاك و بەردەستن کە ئیمە وەك بەرنامە Softwareدەیان ناسین. سۆفت وێر Softwareزاراوەیەکی گشتی یە بۆ هەموو ئەو بەرنامانەی All Programs کە بەردەستە و

دەتوانین بەهۆیەوە فرمانەکان جیبەجێبکەین.

لەگەڵ بەرەو پێشچوونی تەکنەلۆژیا، نەوەی نوێی بەرنامەکان بڵاوکرایەوە، بەڵام پێویستە ئاگاداری ئەوە بین کە ئەو دۆکۆمینتەی Documentبەنەوەی نوێ درووستکرابێت بەنەوەی کۆن ناکرێتەوە، لەبەرئەوەی نەوەی کۆن هەموو توانا و لێهاتوویی‌یەکی پێویستی نی یە بۆ کردنەوە و جێبەجێکردنی دۆکۆمێنتۆکە.

سۆفتوێر Softwareکۆمەلێك بەرنامەیە Programs، کە نەخشەسازی کراوە بۆ جێبەجێکردنی کارێکی دیاری کراوی تەواو، بەرنامەش بریتییە لە زنجیرەیەك رێنمایی و فرمانی نووسراو بۆ چارەسەر کردنی گرفتێکی دیاری کراو.

بەرنامەکان بە شێوەیەکی گشتی دوو جۆرن، کەلیرەدا بەتەواوی باسیان دەکەین:

١. بەرنامەی نەزم – System Software.
٢. بەرنامەی جێبەجێکردن – Application Software

بەرنامەی نەزم – System Software

بەرنامەی سیستەم System Software کۆکراوەی کۆمەلێك بەرنامەیە Collect of Programs کە نەخشەسازی بۆ کراوە بۆ کار Operate، دەست بەسەراگرتن و چاودێری Control، و درێژکردنەوەی توانا و لیهاتووی چارەسەرکردنی کۆمپیوتەر، بەرنامەی سیستەم System Software ئامادە دەکرێت لەلایەن کارگە و کۆمپانیاکانی بەرنامەوە Software Manufacture، ئەم بەرنامانە بەرهەمی تەواوی بەرنامەکانە Programs کە نووسراوە بە زمانە ئاست نزمەکان Low – Level Language، کە کارلێکدەکات Interact لەگەڵ ئامێرەکان Hardware لە ئاستێکی زۆر بنچینەیی Very Basic Levelدا. خزمەتگوزارییەکانی بەرنامەی سیستەم System Software وەکو رووکارێك Interface وایە لە نێوان پارچە رەقەکان (ئامێرەکان) و بەکارهێنەر User.

هەندێك نموونەی بەرنامەی سیستەم System Software ئەمانەن :

١. سیستەمی کارپێکردن Operating System.
٢. وەرگێرەکان Compilers.

٣. ڕاڤەکارەکان (مـوفەسیرەکان) Interpreters.

٤. ئەسیمبلّەرەکان Assemblers.

سیستەمی کارپێکردن – Operating System

سیستەمی کارپێکردن Operating System گرنگترین بەرنامەیە کە جێبەجێدەبێت لەسەر کۆمپیوتەر، ئەم بەرنامەیە یادگەی کۆمپیوتەر Computer's Memory و پرۆسێسەکان Processes ، هەموو بەرنامەکان All Software و پارچەرەقەکان (ئامێرەکان) بەڕێوەدەبات.ئەم بەرنامەیە ڕێگە بە گەیاندن و پەیوەندیمان دەدات بە کۆمپیوتەرەوە بە بێ ئەوەی بزانین چۆن زمانی کۆمپیوتەر قسە دەکات.

کاری سیستەمی کارپێکردن The Operating System's Job

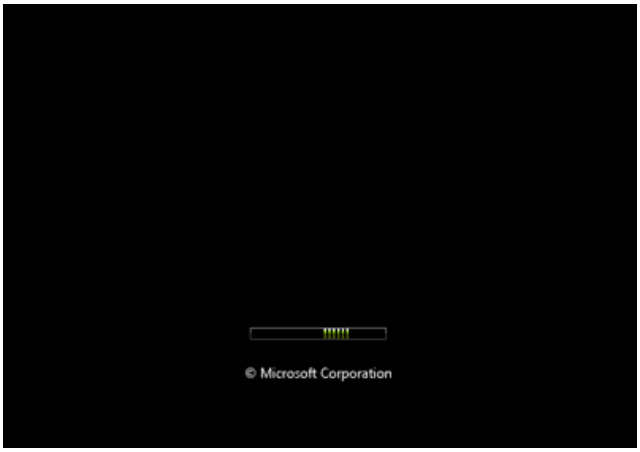
کاتێك باس لە سیستەمی کارپێکردنی کۆمپیوتەر دەکرێت، گوێمان لەوە دەبێت کە سیستەمی کارپێکردن کۆمپیوتەرەکەمان ئامادە دەکات و کارپێدەکات Boot Your Computer ، بەڵام دەتەوێت بزانی مەبەست لەمە چی یە ؟ ئامادەکردن و کارپێکردن Booting بریتییە لەو پرۆسەیەی کە ڕوودەدات کاتێك پەنجە دەنێین بە دووگمەی داگیر ساندنی کۆمپیوتەر Power، بۆ کارپێکردنی کۆمپیوتەرەکەت، کە لەم ماوەیەدا یەك بۆ دوو دەقەی پێدەچێت و، کۆمپیوتەر چەند کارێك ئەنجام دەدرێت:

١. تاقیکردنەوە و پشکنین جێبەجێدەکات بۆ دڵنیابوون لەوەی هەموو شتەکان بەرێکی کار دەکات.

٢. پشکنین دەکات بۆ ئامێر و پارچەی ڕەقی نوێ.

٣. دەستکردن بە کارپێکردنی سیستەمی کارپێکردن.

لەکار پێکردندا ئەم ڕووکارەی خوارەوە دەردەکەوێت :



دووەم// پارچە رەقەکان ((ئامێرەکان)) Hardware:

ئامێرەکان یان پارچە رەقەکان تەکنەلۆژیایی فیزیایین Physical Technology، کە مالّ و شوێنی جیبەجێکردنە بۆ بەرنامە Software، پاشەکەوت کردن Store، هەلّگرتن و گواستنەوەی زانیاری Carrier، هەروەها رووکارێك Interface دابین ئەکات بۆ داغلّکردن و وەرگرتنەوەی زانیاری لە سیستەم دا.

پاراستنی فیزیکی Physical Securityدەگەرێتەوە بۆ ئامێر و پارچە رەقەکان، ئامرازە کۆنەکانی جیبەجێکردنی پاراستن کە بە شێوەی فیزیکین، وەکو قوفلّ و کلیل، کە بەکاردێن بۆ پاراستنی بەشە پێکهێنەرەکانی سیستەمی زانیاری.

تێگەیشتن لە زاراوەی هارد وێر

Understand the term hardware

پێناسەیەکی باو و بلّاو ئەوەیە کە، هارد وێر Hardware بریتییە لە بەشی پێکهێنەری ئەلیکترۆنیکی Electronic Components، بۆردەکان Boards، لاوەکی و ڕووکارەکان Peripheral، و ئامێرەکان Equipment. کە سیستەمی کۆمپیوتەر دروست دەکەن، بە پێچەوانەی بەرنامەوە Software، کە بەم پارچانە دەلێن چی بکەن؟؟.

یەکەی سیستەم The System Unit: بریتییە لە سندوقی سەرەکی Main Box کە بەشە ئێلیکترۆنیکییە سەرەکییەکانی تێدایە، وەکو بۆردی دایك Motherboard، چارەسەر کەر Processor، کارپێکەری هارد Hard Drive، ڕام RAM-Random Access Memory.

ئامێرە ڕووکارەکان ((لاوەکییەکان)) Peripherals: **هەموو ئەو ئامێرانە** All Devices **دەگرێتەوە، کە دەکرێن بە** Plug into **یەکەی سیستەمەوە** System Unit. **ئەم ئامێرانە لەوانەیە داغڵکەر** Input **یان بەرهەم** Output **بن.**

نوێکردنەوەی بەشی پێکهێنەر بۆ هاردوێر وەکو درایڤەر Driver**، لە کاتێکەوە بۆ کاتێکی تر دڕووست دەکرێت لەلایەن کارگەکانەوە بۆ هاردوێرەکان.**

سێهەم//زانیاری شیکارنەکراو Data:

زانیاری شیکار نەکراو پاشەکەوت دەکرێت Store، چارەسەر ((شیکار)) دەکرێت Process، دەگوێزرێتەوە لە رێگەی سیستەمی کۆمپیوتەرەوە و، پێویستە ئەم زانیارییە لە هەموکات و شێوەکان دا بپارێزرێت، چونکە زانیارییەکان نرخ و گرنگییان هەیە و، بەم هۆیەوە دەبنە ئامانج بۆ هێرش کردنە سەریان.

لە بابەتەکانی سەرەتادا، بەوردی باسی داتامان کردووە و، لەگەڵ زانیاری بەراوردمان کردووە و، لێکچوون و جیاوازییەکانیانمان خستۆتە روو، هاوکات هەنگاوەکانی گۆڕیتی داتا Data بۆ زانیاری Informationمان خستۆتە روو.

چوارەم//خەڵک People:

خەڵک وەک بەکارهێنەر و بەڕیوەبەری سیستەمی زانیاری و، وەک هێرشبەریش بۆسەر سیستەمی زانیاری کە دەبنە هەرەشە بۆ سیستەمی زانیاری، لە دیارترین بەش و پێکهاتەکانن و، پاراستنی زانیاری بۆئەم حاڵەتە زۆر گرنگ و پێویستە تا زانیاری نەفەوتێت، یان نەکەوێتە دەست ناحەز و دووژمن و نەبێتە مایەی گرفت و کێشە بۆ سیستەمی زانیاری.

پێنجەم//شێوە و پەیرەوی جیبەجێکردن Procedure:

یەکێک لە بەشە پێکهێنەرە گرنگەکانی تری سیستەمی زانیاری بریتی یە لە شێوە و پەیرەوی جێبەجێکردن Procedure، کە نووسینی فرمانەکانە بۆ جیبەجێکردن و تەواو کردنی کارێکی دیاری کراو، کاتێک کەسێکی رێگە پێنەدراو شێوە و پەیرەوی جیبەجێکردنی رێکخراوێک وە دەست دەخات، ئەوا دەبێتە هەرەشە بۆسەر سەلامەتی زانیاری Integrity of Information.

لەبەر ئەوە زانیاری فەرمانبەر لە بارەی پاسەوانی Safeguarding شێوە و پەیرەوی جیبەجێکردنەوە Procedure بریتییە لە گرنگترین خاڵی پاراستنی سیستەمی زانیاری.

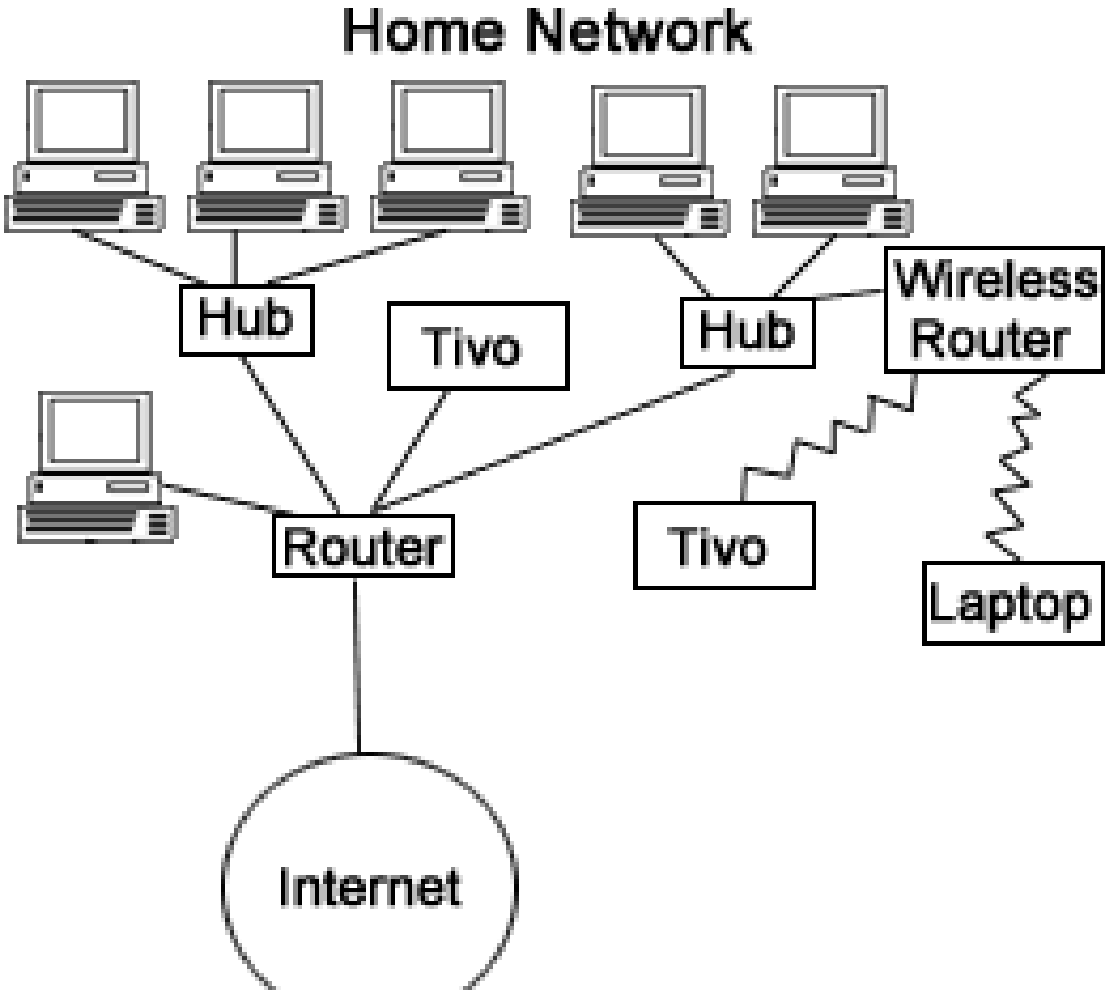
بەڵام ناساندنی و شیکردنەوەی شێوە و پەیرەوی جیبەجێکردن Procedure بە گوێرەی بەرنامەسازی و بنکەی زانیاری کەمێک جیاوازە و دەگۆڕێت، بۆیە ئەو پێناسانەش دەخەینە روو:

- لە بەرنامەسازی کۆمپیوتەر دا Computer Programming، شێوە و پەیرەوی جیبەجێکردن Procedure کۆمەلێك لە فرمانە بەکۆدکراوەکانە Coded Instructions کە بە کۆمپیوتەر دەلێت چۆن بەرنامەیەك جیبەجیبکرێت ، یان کردارێکی ژمێرەیی ئەنجام بدرێت. ژمارەیەکی زۆر و جیاواز زمانی بەرنامەسازی کۆمپیوتەرمان هەیە، کە دەتوانین بە کاریان بهێنین بۆ دروستکردنی پەیرەوی جیبەجێکردن Procedure، بە پشت بەستن بە زانەکانی بەرنامەسازی، ئەم شێوە و پەیرەوی جێبەجێکردنە پێی دەلێن : رۆتین Subroutine، نیمچە بەرنامە subprogram یان کردار Function.
- لو بەرنامەسازی بنکەی زانیاری Database Programmingدا، شێوە و پەیرەوی جیبەجێکردن Procedure کۆمەلێك لە کۆدی بەرنامە سازی یە Programming Code وەکو PL/SQL، کە پرسگە Query یان کردارێکی Function دیاری کراو جیبەجێدەکات، ئەم پەیرەوە Procedure پاشەکەوت کراوە Stored بەکاردێت بۆ جێبەجێکردنی یەك یان کۆمەلێك فرمان Command، گەران بۆ Search For، خستنە ناو Insert، نوێکردنەوە Update یان سرینەوە Delete ی زانیاری لە بنکەی زانیاری دا.

شەشەم/ڕایەڵە Networks:

یەکێك لە بەشەپێکهێنەرە گرنگەکانی تری سیستەمی زانیاری بریتی یە لە رایەڵە ((تۆر – نیتۆرك))، رایەڵە بریتی یە لە کۆکروەی کۆمپیوتەرەکان Computers، راژەکارەکان Servers، مەینفرەیم Mainframe ، ئامێرەکانی رایەڵە Network Device، ئامیرە لاوەکییەکان Peripherals، یان هەر ئامێرێکی تر، پێکەوە بەستراون بۆ گواستنەوە Transfer و بلاوکردنەوە Share و بەکارهێنانی use زانیاری گەورەترین نموونەی رایەڵە ئینتەرنێتە Internet، کە ملیۆنەها کەسی پێکەوە بە ستۆتەوە.

بەڵآم کاتێك سیستەمی زانیاری پێکەوە گرێدەدرێن بە شێوەیەکی ناوچەیی لە تۆری ڕووبەری ناوچەیی LAN Local Area Networkدا، یان لەگەل سیستەمی زانیاری تر لە دەرەوە و لە دوورەوە بە هۆی ئینتەرنێتەوە لە شێوەری تۆری ڕووبەری فراوان WAN Wide Area Network، ئەوا زیاتر پێویستمان بە پاراستنی زانیاری دەبێت Information Security بۆ ئەم سیستەمی زانیاری یە.



پاراستنی نێتوێر

Netware Security

نێتوێر NetWare، لە هەر دوو وشەی رایەڵە Network و، بەرنامە Software وەرگیراوە، نێتوێر NetWare بریتی یە لە سیستەمی کارپێکردنی رایەڵە Network Operating System، کە بۆیەکەم جار ناسێنرا لە لایەن نۆڤێڵ Novellـــــەوە.نێتوێری نۆڤێڵ Netware Novell یەکەم بەرنامەی لان LAN Software بوو، لەسەر بنچینەی تەکنەلۆژیایی راژەکاری فایل File Server Technology، کە لەسەر هەردوو ئیسەرنێت Ethernet و رایەڵەی ئای بی ئێم IBM Token – ring Network جێبەجێدەبێت.

هێرشەکانی پاراستن

Security Attacks

کاتێك سیستەمی پاراستن Security System بنیات دەنرێت و دروست دەکرێت، رووبە رووی هەندێك کێشە دەبێتەوە و دەبێتە گرفتی گەورە بۆیی، رەنگە وای لیبکات کە پاراستن لە دەست بدات، یاخوود ئاست و جۆری پاراستن کەم ببێتەوە بە هۆیەوە، ئەویش بریتییە لە هیرشەکانی سەر سیستەمی پاراستن. کە لیرەدا زۆر بەکورتی و بە گویرەی پیویست باسیان دەکەین.

یەکەم// مالۆیر

Malware

مالۆیر Malware هەر کۆدێکی کۆمپیوتەرە Computer Code،کە بۆ مەبەستێکی خراپ و پیس Malicious بەکاردێت، مالۆیر بەکاردەهێنرێت بۆ تێکشکاندنی Destroy هەنێ شت لە کۆمپیوتەر دا، یان بۆ دزینی زانیاری تایبەتی.

مالویرەکان وەکو ڤایرۆس Virus و، ئەسپی تەروادە Trojan Hoarse و سپای وێر Spy Ware و ..... . لیرەدا تەنها بە کورتی باسمان کرد و، لە بەشێکی سەربەخۆ دا، بەوردی باس لە مالویر و جۆرەکانی دەکەین.

دووەم// لە پشتەوە (دەرگەی پشتەوە)

Back Door

بەشێوەیەکی گشتی ناسراوە وەکو دەرچە Trap Door، یان مەنهۆل ((درزی داغڵبوون) Manhole، لە پشتەوە Back Door زاراوەیەکە بەکاردەهێنرێت بۆ وەسفکردنی رێگەی پشتەوە Back Way، رێگەی شاراوە ((پەنهان)) Hidden Method، یان هەر شێوەیەکی تری تێپەراندنی پاراستن بۆ بەدەست هێنان Gain و دەستپێگەیشتنی Access زانیاری.

کەواتە دەتوانین بڵێین: پارچەیەك کۆدی بەرنامەی نووسراوە Piece of Program Code، لە بەرنامەی

جیبەجێکردن Application یان سیستەمی کارپێکردن Operating Systemدا، بۆ پێبەخشین و پێدانی Grant دەستپێگەیشتن Access بە بەرنامە ساز Programmer بە بێ ئەوەی پێویستی بە تێپەرین هەبێت بە خاڵی ئاسایی دەست بەسەراگرتنی پاراستنەوە.

سێهەم // هێرشی بێهەستی بەهێز

Brute Force Attack

هێرشی بێهەستی بەهێز Brute Force Attack تەکنیکێکە بۆ بەزۆر یان لەپر گرتنی Capture نامە و پەیامی بەکۆد کراو Encrypted Message، بۆ تێکشکاندنی کۆد و ، بەدەستهێنانی دەست پێگەیشن Gain Access، ئای دی بەکارهێنەر User ID، و تیپەرە وشە Password.

هێرشی کریپتۆگرافی Cryptography Attack و تیپەرە وشە Password Attack هەوڵدان نی یە بۆ گۆرینی کۆدە بۆ شێوەی ئاسایی Decrypt، بەڵکو بەردەوام بوون و هەوڵدانە بۆ دروستکردنی لیستێکی جیاوازی تیپەرە وشە Password، وشە Word، و پیت Letter. بۆ نموونە لەوانەیە هێرشی بێ هەستی بە هێز Brute Force Attack فەرهەنگێك بێت لە هەموو ئەو وشە باوانەی Commonly Word بە کاردەهێنرێن بۆ تیپەرە وشە Password، لە رێگەی ئەم وشانەوە هەوڵدەدرێت هەتاوەکو دەستی بگات بە ئەژمارەکە Account، بەلام ئەمە جۆری سادەیی هێرشی بێ هەستی بەهێزە Brute Force Attack، دەکرێت ئەم هێرشە چەند کاتژمێرێك بخایەنێت، یان چەند رۆژێك ، یان چەند مانگێك و تەنانەت چەند ساڵێکیش. ئەمەش دەگۆرێت و پشت دەبەستێت بە ئالۆزی تیپەرە وشەکە Complexity of Password ، بەهێزی شاردنەوە Strength Encryption.

چوارەم// هێرشی بێبەشکردن لە خزمەتگوزاری

Denial of Service Attack

هێرشی بێبەشکردن لە خزمەتگوزاری Denial of Service Attack ، یان هێرشی دۆس DOS Attack، شالاو بردنە بۆ سەر کۆمپیوتەرێکی تر، یان یان کۆمپانیایەك بە ناردنی Sending ملیۆنان Millions یان داواکاری زیاتر More Request لەهەر چرکەیەك دا، کە ئەمەش دەبێتە هۆکاری

پەککەوتنی رایەڵە Network Down بە هیواشی، یان دەبێتە هۆی هەڵە Error و کوژاندنەوە Shut Down.

کەواتە دۆس DoS ئەو شالاوەیە Attack، کە مەبەست لێی بەدەستهێنانی دەستپێگەیشتن Access نی یە، بە رایەڵە Network یان سیستەم System، بەڵکو ئامانج پچراندنی Disrupting خزمەتگوزاری رایەڵە Network یان سیستەمە System. ئەم هێرشە Attack لەوانەیە لەسەرچاوەیەکە One source یان زیاتر لە سەرچاوەیەکەوە Multi Source بێت.

پێنجەم// خراپ کەڵکلیوەرگرتن

Exploiting

خراپ کەڵکلێوەرگرتن ((ئیستیغلال کردن)) Exploit، بەرنامەیەکە Program یان کۆمەلێك فرمانە و ، ئامادەکراوە و نەخشە سازی بۆ کراوە بۆ ئەوەی هێرش بەر Attacker بەکاری بهێنێت تا بەهۆیەوە خاڵی لاوازی بەرنامە و پاراستن Vulnerability، بدۆزێتەوە، و بە خراپ کەڵکی لیوەربگرێت و بەکاری بهێنێت.

خاڵی لاوازی پاراستن Security Weakness، لەبەرنامەدا، دەبێتە هۆی تێخزاندنی بەرنامە و کۆدی زیان بەخش لە لایەن هێرش بەرەوە بۆ ئەوەی لەکاتی بەکارهێنانی ئەو بەرنامەیەدا، بە خراپ کەڵکی لێوەربگیرێت، وەك سوود وەرگرتن لە خاڵی لاوازی وێبگەر Web Browser ، یان رێگە دان بە خوێندنەوە یان لەبەر گرتنەوەی فایلەکانت.

شەشەم // هەلهێنانی تێپەرە وشە

Guessing Password

هەلهێنانی تیپەرەوشە Guessing Password، تەکنیکێکە بە بەکارهێنانی بەرنامە بۆ تاقیکردنەوی هەموو گریمانەکان بۆ هەلهێنانی تیپەرەوشە و، بەدەستهێنانی توانای داغڵبوون، بۆ ناو سیستەمێك یان رایەڵە.

ناوی بەکارهێنەر و تێپەرە وشە

User Name & Password

زۆربەی سیستەمەکانی کارپێکردن، وەکو مایکرۆسۆفت ویندۆز دەتوانرێت ناوی بەکارهێنەر و تێپەرە وشەی پێبدرێت بۆ ناسینەوەی بەکارهێنەر، بۆ ئەوەی بزانرێت ئەوەی داغڵ دەبێت کێیە؟ یاخود بۆ دیاری کردنی سنووری بەکارهێنەر و ئەو کەسەی داغڵدەبێت بە هۆی کۆنترۆڵی باوانەوە Parental Control، بۆ دڵنیابوون لە ریبەر و سنووری داغڵبوو ((بەکارهێنەر))، ئەمەش رووەدات بە بەکارهێنانی یەك بەکارهێنەر ((داغڵبوو Login، یان ئای دی ID))، بە بەکارهێنانی ناو Name و وشەی تێپەڕ Password.

لە هەر شوێنێکدا کە چەند کۆمپیوتەرێك پێکەوە گرێدەدرێن، یان دەکرێنە رایەڵە Networked، وەکو لە خوێندنگە یان شوێنی گەورەی کارکردن، بەکارهێنەری داغڵبوو دەتوانرێت سنوور داربکرێت و پێوەندی بۆ دابنرێت، یان هانی ئاڵوگۆری زانیاری پارێزراو بدرێت لە رایەڵەکەدا. رێسا و یاسایی دەستپێگەیشتن زۆر گرنگە، بۆ ئەوەی هیچ کەس نەتوانێت وەك تۆ و بەناوی تۆوە داغڵ ببێت. چونکە توانایی کردنەوە Open، خوێندنەوە Read، سرینەوە Delete، گۆرین Change و بڵاوکردنەوە Publish ی دۆکۆمێنت Document بەناوی تۆوە و لە ژێر ناسنامەی تۆدا. مەترسیدارە ... !!!

پێوەرەکانی تێپەرە وشەی باش

Good Password Criteria

تیپەرە وشەی باش و گونجاو، بۆ ئەوەی لە هەرەشە و دزین دووربێت و بە ئاسانی دەست کەسی بێگانە نەکەوێت، پێویستە رەچاوی پێوەرەکان بکرێت، کە بە کورتی ئاماژەیان پێدەکەین:

١. تێپەرە وشە Password پێویستە ئاسان بێت بۆ بیرکەوتنەوە، بەڵام سادەنەبێت بۆ ئەوەی بە ئاسانی دەست هێرش بەرەکان Attackers نەکەوێت.
٢. پێویستە لانی کەم، تێپەرە وشە هەشت کارەکتەر Character بێت.
٣. هێما و پیتەکان و ژمارەکانی تێدا بەکاربێت بە تێکەڵ و پێکەڵی بۆ ئەوەی بە ئاسانی نەدۆزرێتەوە و نەکەوێتە بەردەست هێرش بەرەکان.
٤. هەندێك تێپەرەوشە Password وردکارە Case Sensitive، مەبەست لەوەیە کە جیاوازی

دەکات لەنێوان گەورە Capital و بچووك Small، ئەمەش بە سوودە بۆ زیاد کردنی پاراستن.

٥. گۆرینی تێپەرەوشە Password بەشێوەیەکی رێك و گونجاو و ، ماوەوە.

٦. پێویستە تیپەرە وشە بلاونەکردێتەوە لەگەڵ هیچ کەسێکی تر و، نەدرێت بەکەس. تەنها خۆمان بیزانین و بەس.

کارتی زیرەك

Smart Card

کارتی زیرەك Smart Card، کارتێکی پلاستیکییە Plastic Card، بە شێوەیەکی گشتی حەجمەکەی وەکو کاری دڵنیایی Credit Card وایە، لەگەڵ بوونی پارچەیەکی ئەلیکترۆنی بچووك Microchip لەسەر ی کە زانباری پێویست و گرنگی لەسەرە و دەتوانرێت لێی وەربگیرێتەوە هەر کات پێویست بوو.

دەتوانرێت بەکاربهێنرێت بۆ پەیوەندی تەلەفۆنی Telephone Call، پارەدانی ئەلیکترۆنی Electronic cash payment، دەستگەیشتن بە نامەی ئەلیکترۆنی E-Mail Access، زۆر بەرنامە و جیبەجێکردن دەکرێتەوە بە بەکارهێنانی کارتی زیرەك، و پی ئای ئێن PIN((ژمارەی ناسینەوەی کەسی Personal Identification Number)) یان تێپەرەوشە Password، بۆ دڵنیابوون لە ساغکردنەوە ((مۆرکردن)) Authentication.

شکێنەری تێپەرەوشە

Password Cracker

شکێنەری تێپەرە وشە Password Cracker، بەرنامەیەکە کە تیپەرەوشە دەگیرێتەوە بۆ شێوەی ئاسایی خۆیی و لە هێماوە دەیکاتەوە بەو شێوەیەی لێی تێبگەین، واتە بە کۆد کردنی تێپەرەوشە ******** لادەبات Decrypt، پاراستنی تیپەرەوشە ناهێلێت و لای دەبات. رێگە بە داغڵبوون و دەست گەیشتن بە زانیاری تایبەتی Private و نهێنی Confidential دەدات.

شکێنەری تێپەرە وشە Password Cracking بۆ کەمەلێك مەبەست بەکاردەهێنرێت:

١. یارمەتی بەکارهێنەر دەدات بۆ هێنانەوە Recovery ی تێپەڕەوشەکەی لەکاتی لەبیرکردنی دا.
٢. بۆ بەدەستهێنانی دەستپێگەیشتنی ڕێگەپێنەدراو Unauthorized Access، بە شێوەیەکی نایاسایی. ئەمەش مەترسییە بۆ سەر زانیاری ڕێکخراوە و حکومی و دام و دەزگاکان.
٣. بۆ لابردن و گێڕانەوەی تیپەرە وشە بۆ شێوەیەك کە بخوینرێتەوە و بتوانرێت بناسرێتەوە و سوودی لێوەر بگیرێت بۆ داغڵبوون.

جۆرەکانی تیپەرە وشە

Password Types

تیپەرە وشەکان دەکرێت بە چەند جۆرێکەوە و، هەریەکە و لە ڕووی پاراستنەوە جیاوازی هەیە و، لە ڕووی تایبەتمەندیشەوە جودایە، بۆیە پێویستە شارەزایمان هەبێت لە بارەیانەوە:

١. تیپەرە وشەی بەهێز Strong Password :

ئەو تیپەرە وشەیە یە کە چەند مەرجێکی بەسەردا جیبەجێ ببێت و، ئەم خالانەی لای خوارەوە تیادا بێت:

- کارەکتەری بەهەردوو شێوەی گەورە Upper case و بچووك Lower Case تیابێت. وکو((A,a,x.X, ...)).
- ژمارەکان Digits و هێماکانی خاڵبەندی Punctuation لەخۆ بگرێت وەکو پیتەکان Letter، بۆ نموونە ((/ , ? ; <> : " [] {} = - + _ () * & ^ % $ # @ !|)).
- لانی کەم هەشت ((٨)) کارەکتەر بێت.
- وشەی تیانەبێت وەك وشەکانی هەر زمانێك یان لەهجەیەوەك ((کورد، کوردستان، هیمن، ساڤۆ،هەناسە، هەستی، راز، .....)).
- تیپەرە وشە Password نابێت لەسەر بنەمای زانیاری کەسی بێت، وەکو ((ناو و ناوی خێزانی – هێمن، بەرزنجی، کەریم، مەلا، مەلا کەریم، .....)).

٢. تیپەرەوشەی لاواز Weak Password:

تیپەرە وشەی لاواز Weak Password دەبێتە مایەی گرفت و ئاستی پاراستنی زانیاری دادەبەزێنێت و، ڕەنگە بە سانایی زانیاری بکەوێتە دەست کەسانی ناحەز و خراپە کار ، بۆیە پێویستە ئاگاداربین و تیپەرە وشەی لاواز هەلنەبژێرین، ئەم خالانەی لای خوارەوە ڕوونی دەکەنەوە کە چ کاتێك تێپەرەوشەیەك لاوازە:

- کەمتر لە هەشت کارەکتەر.
- وشەکە لە فەرهەنگ Dictionaryدا هەبێت و بدۆزرێتەوە.
- زاراوەکانی کۆمپیوتەر و ناوەکان، فرمانەکان، مالپەڕەکان، کۆمپانیاکان، پارچەڕەقەکان، ئامێرەکان، بەرنامەکان، و یانە وەرزشییەکان.
- بەروار و رۆژ و مانگی لە دایك بوون، یان هەر زانیارییەکی تری کەسی وەك ژمارە مۆبایل، ناونیشان، .....
- وشە یان ژمارەی شێوە نەخش و دووبارە و ئاسان وەکو ((١ ٢ ٣ ٤ ٥ ٦ ٧ ٨، aaaabbbb، .....)).

بە ئاسانی توانای هاککردنی هەیە

Easily Hackable

هەندێك تیپەرە وشە بە ئاسانی هاك دەکرێت، واتە بە ئاسانی دەکەوێتە دەست کەسی بەرامبەر بۆیە پێویستە ئەو جۆرانە بناسین و، خۆمان بە دوور بگرین لێیان، بە کورتی لێرەدا ئەو جۆرانە دەخەینە روو:

یەکەم// بەکارهێنانی تیپەرە وشەی سادە- Use a Simple Password:

بەکارهێنانی تیپەرە وشەی سادە و باو، یەکێکە لەو جۆرانەی تیپەرە وشە کە بە ئاسانی دەشکێنرێت یان دەکەوێتە دەست بەرامبەر و، هاك دەکرێت، بە شێوەیەکی گشتی ئەم تیپەرە وشانە ی لای خوارەوە سادەترین و باوترینن کە لەهەموو جیهانا لەلایەن بەکارهێنەرانەوە بەکار هاتووە:

1. 123456
2. 12345
3. 123456789
4. password
5. iloveyou
6. qwerty
7. rockyou
8. 1234567
9. 12345678
10. abc123

دووەم// بەکارهێنانی تیپەرە وشەیەك كە هەلهێنانی ئاسانە Use a Password that's Easy to Guess:

پێویستە ئەو تیپەرە وشانە بەکارنەهێنرێت کە هەلهێنانی ئاسانە و بە زووی و بە ئاسانی دەدۆزرێتەوە، وەك لە بابەتی لاوازی تیپەرە وشەدا رووننمان کردۆتەوە، چونکە تیپەرە وشەی لاواز بە ئاسانی هەلەهینرێت و ئەدۆزرێتەوە.

سێهەم// رۆژی هاوسەرگیری و لە دایك بوون Wedding & Birth Day:

یەکێك لە تیپەرە وشە لاوازەکانی تر کە زۆر بەکار دەهینرێت، رۆژی هاوسەر گیری یان رۆژی لەدایك بوونە و ، ئەمەش گرفتە و بە ئاسانی هاك دەکرێت و دەکەوێتە دەست بەرامبەر .

چوارەم// بەکارهێنانی هەمان تیپەرە وشە لە چەند مالپەرێك دا Use the Same Password on Many Web Site:

بەکارهێنانی یەك تیپەرە وشە بۆ چەند ئەژمارێك لە چەند مالپەرێك دا، بە ئاسانی بیر دێتەوە و، بەکارهێنەریش سوودی لیوەر دەگریت بۆ ئەو بیر هێنانەوەیە، بەلام ئەمە گرفت دروستەکات و ئەگەر بکەوێتە دەست بەرامبەر و ناحەزران ئەوا هەموو ئەژمارەکان Account دەکەوێتە مەترسییەوە.

تیپەرە وشە و ... سیستەمی کارپێکردن

Password & Operating System

سیستەمەکانی کارپێکردن بە هۆی تیپەرەوشەوە Password دەپارێزرێن، وەك ئاستێکی پاراستنی زانیاری، بۆ نموونە لە سیستەمی کارپێکردنی ویندۆز Windowsدا، لێرەدا وەك نموونەی کرداری دەیهێنینەوە بۆ هەردوو ویندۆزی حەوت و هەشت. چونکە دوو جۆری باوی کوردستانن. هەروەها باس لە جۆرەکانی ئەژمار Account دەکەین وەکو پاڵپشتی ئەم پاراستنە و، دەستبەسەراگرتنی باوان Parental Control بۆ زیادکردنی ئەم پاراستنە Security.

جۆرەکانی ئەژماری بەکارهێنەر

Account Types

پێش ئەوەی ئەژمارێك دابنێین، پێویستە جۆرەکانی ئەژماریش بزانین، چونکە جۆرەکانی ئەژمار دەبێتە تەواوکەری تیپەرە وشەکە و بەهۆیەوە ئاست و سنووری بەکارهێنەر دیاری دەکرێت:

١. ئەژماری پێوانەیی Standard Account، ئەو ئەژمارە بنچینەییانەیە کە بەکاردێت بۆ شێوە ئاساییەکان، کار و باری رۆژانەوەکو بەکارهێنەری پێوانەیی دەتوانیت هەموو ئەو کارانە بکەیت کە پێویستە بیکەیت، بۆ نموونە کردنەوەی بەرنامە، رێکخستنی سەر شاشە. هەروەها دەستبەسەراگرتنی باوان Parental Control لەسەر ئەم جۆرە ئەژمارە دادەنرێت.
٢. ئەژماری بەڕێوەبەر Administrator، ئەژمارە دیاری کراو و تایبەتەکانە کە بەکاردەهێنرێت بۆ گۆڕانکاری لە سیستەم بەشێوەیەکی پارێزراو و دڵنیا، یان بەڕێوەبردنی خەڵکانی تر، ئەژماری بەڕێوەبەر توانای دەست پێگەیشتنی تەواوی هەیە بۆ هەموو رێکخستنەکان و سنووردانانەکان لە کۆمپیوتەر دا.

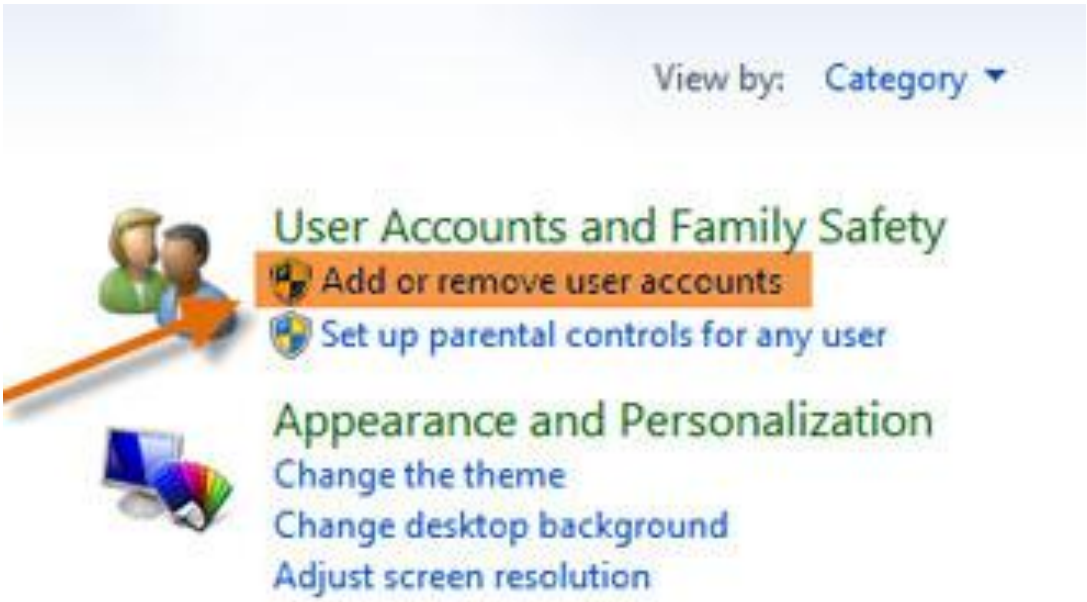
هەر کۆمپیوتەرێك، ڕاژەکار Server بێت یان ڕاژە خواز Client لانی کەم دەبێتە بەڕێوەبەرێکی Administrator هەبێت.

تیپەرە وشە لە ئەژمارەکان دا

Password in Accounts

١. پەنێڵی دەست بە سەرا گرتن Control Panel دەکەینەوە.

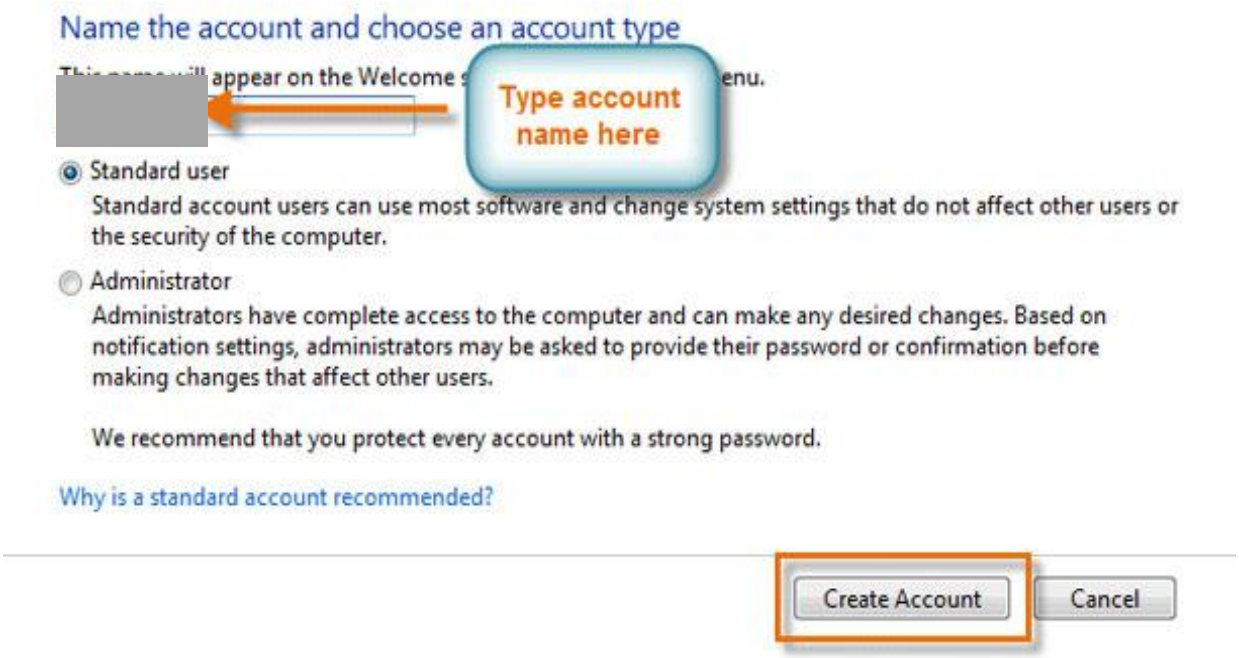
٢. کلیك لەسەر زیادکردن لابردنی ئەژماری بەکارهێنەر Add or Remove User Account دەکەین.



٣. بەشی بەڕیوەبردنی ئەژمارەکان دەکرێتەوە Manage Accounts، هەموو ئەژمارەکان دەبینرێت تیایدا و دەرەکەوێت، کە بەهۆیەوە دەتوانین ئەژماری نوێ دروست بکەین، یان ئەژمارە کۆنەکان بگۆڕین.

٤. بۆ دروستکردنی ئەژماری نوێ New Account، کلیك لەسەر Create New Account دەکەین.

٥. ناوێك بۆ ئەژمارەکە دەنووسین.



٦. یەکێك لە جۆرەکانی ئەژمار ((پێوانەیی، بەریوەبەر)) دیاری دەکەین.

٧. کلیك لەسەر دروستکردنی ئەژمار Create Accountدەکەین.

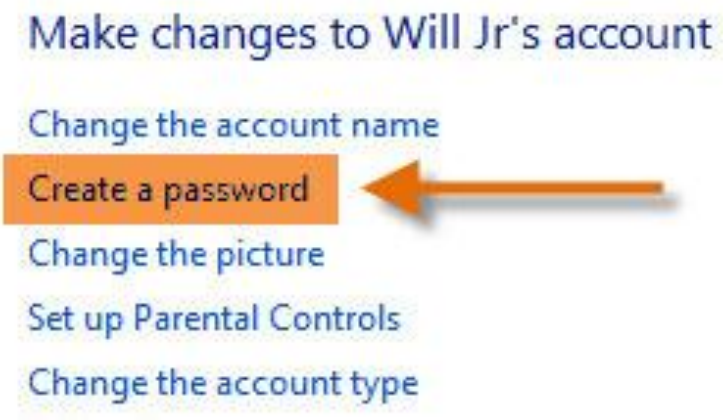
دانانی تیپەرە وشە

To Create Password

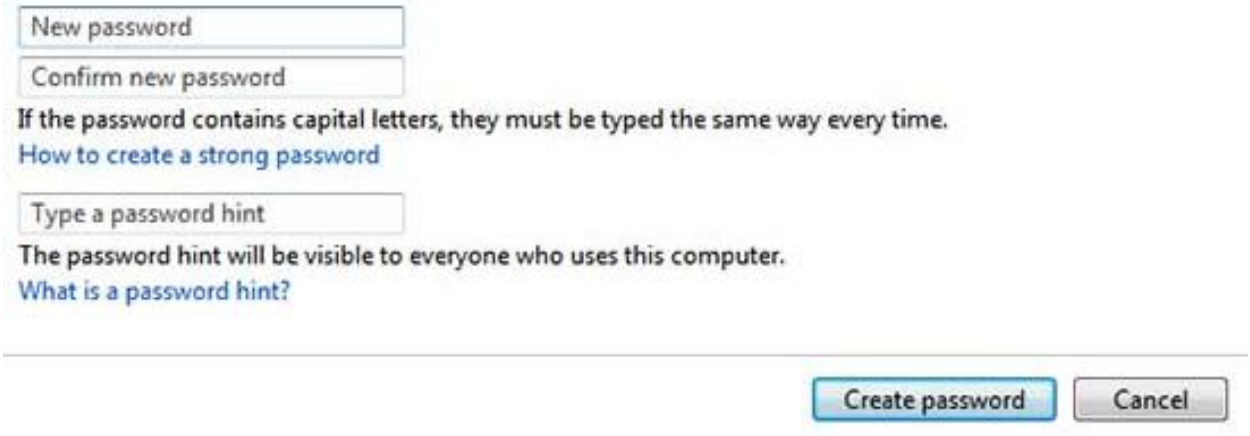
دووای ئەوەی ئەژمارێکمان دروستکرد لە جۆری پێوانەیی Standard پێویستە تیپەرە وشەی بۆ دابنێین بۆ ئەوەی تەنها ئەو بەکاربەرە بتوانێت داخڵ ببێت کە ئەژمارەکەی بۆ دروستکراوە.

١. بەشی بەریوەبردنی ئەژمارەکان دەکەینەوە Manage Accounts، هەموو ئەژمارەکان دەبینرێت تیایدا و دەرەکەوێت، کە بەهۆیەوە دەتوانین ئەژمارە دروستکراوەکە بگۆرین، بۆیە کلیك لەسەر ئەو ئەژمارە دەکەین کە دەمانەوێت تیپەرە وشەی بۆ دابنێین و، پێویستە لە دانانی تیپەرە وشەدا، رەچاوی خاڵەکانی تیپەرە وشەی بەهێز بکەین.

٢. کلیك لەسەر دروستکردنی تیپەرەوشە Create Password **دەکەین.**



٣. لە خانەی تیپەرە وشەی نوێ New Password **دا، تیپەرە وشە داغلّبکە و، لە خانەی پشتراستکردنەوەی تیپەرە وشەی نوێ** Confirm New Password **دا، هەمان تیپەرە وشە دووبارە بکەرەوە بۆ پشت راست کردنەوە.**



٤. کلیك لەسەر دروستکردنی تیپەرە وشە Create Password دەکەین.

دانانی دەست بەسەرا گرتنی باوان

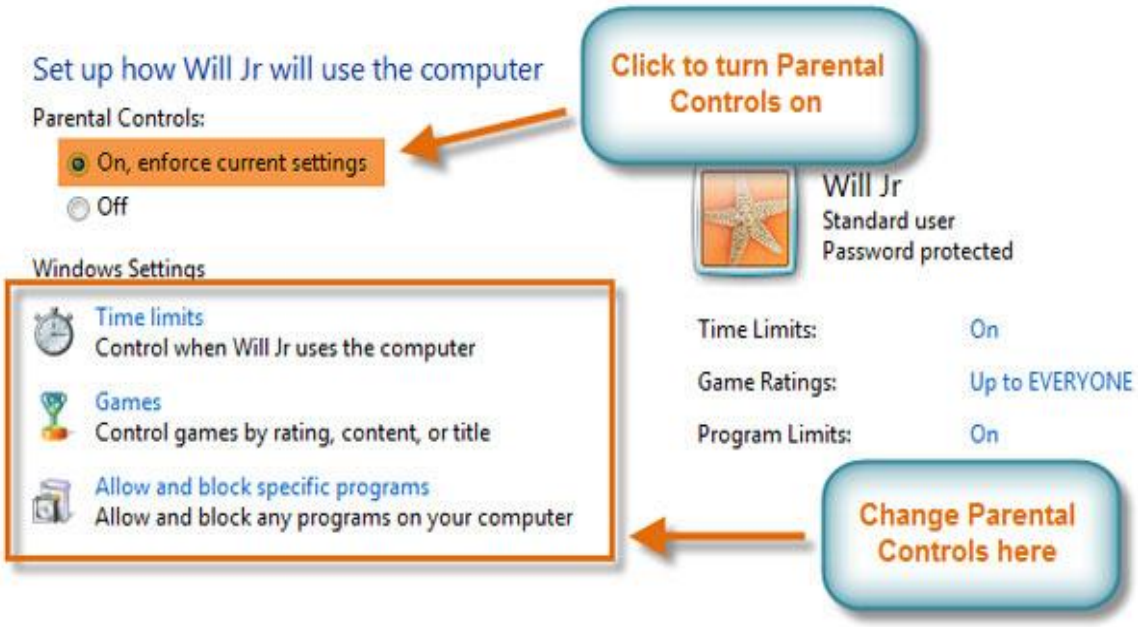
Set Up Parental Control

دانانی تیپەرە وشە بۆ پاراستنە و، بەهۆیەوە ریگە نادەین بەکارهێنەرێکی تر لە جێی بەکارهێنەرێکی تر داغڵبێت، بەلام بۆ دەست بە سەراگرتنی زیاتری ئەم بەکارهێنەرە وابا‌شترە دەست بەسەراگرتنی باوان Parental Control بەکاربەرین. چونکە لە رووی ئاستی بەکارهێنەرەوە پاراستن ئەنجام دەدەین، بۆ نموونە ئەگەر ئەو ئەژمارەی دروستمان کرد بۆ منالێك بێت و بمانەوێت بیپارێزین لە بەکارهێنانی ئینتەرنێت یان یاری یان بەرنامەی تر.

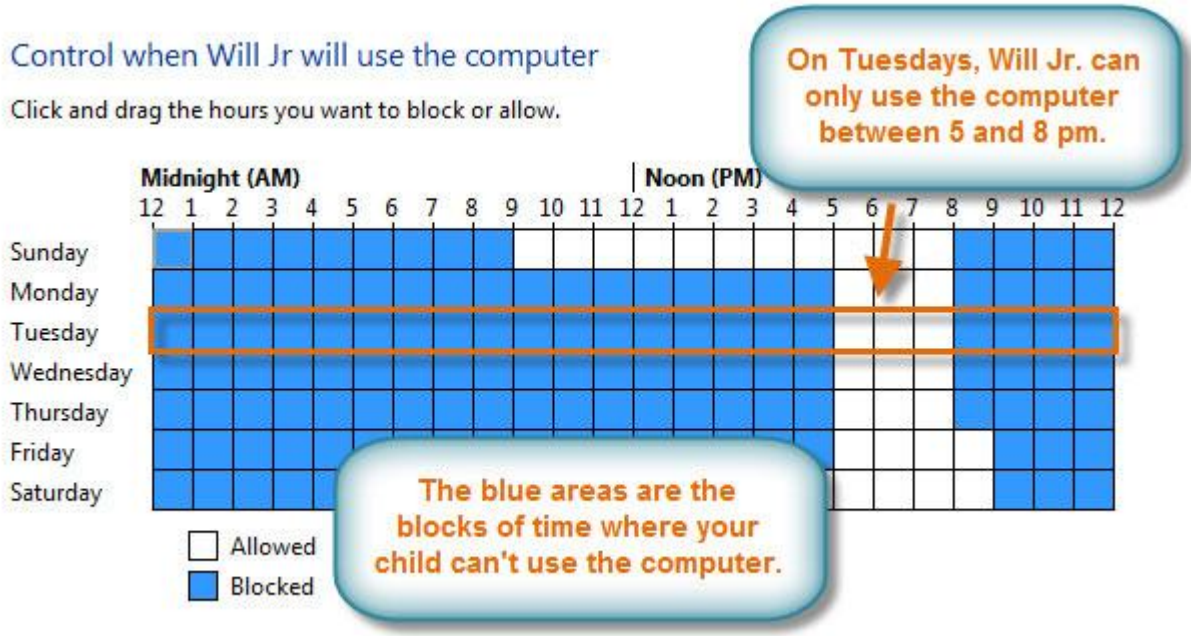
١. پەنیلی دەست بەسەراگرتن Control Panelدەکەینەوە.
٢. کلیك لەسەر دانانی کۆنترۆلی باوان بۆ هەر بەکارهێنەرێك Set up Parental Control for Any Userدەکەین.

٣. هەر ئەژمارێکی پێوانەیی Standard Account هەلەبژێرین بە کلیك کردن لەسەری کە بمانەوێت کۆنترۆڵی باوانی بۆ دابنێین.
٤. کلیك لەسەر دووگمەی رادیۆیی Radio Button کارپێکردنی کۆنترۆلی باوان ئەکەین.
٥. بەهۆیی بەشەکانی دیاری کردن و سنوردار کردنی کات Time Limit، یاری Game و رێگەدان و رێگە نەدان بە بەرنامەی دیاری کراوەوە Allow or Block Specific Software رێگە بە هەر بەرنامەیەك دەدەین کە بمانەوێت ئەم بەکارهێنەرە سوودی لێوەربگرێت و بەکاری بهێنێت و، بە

پێچەوانەشەوە ڕێگری لە هەر بەرنامەیەك ئەكەین كە نەمانەوێ، بەكاری بهێنێت.

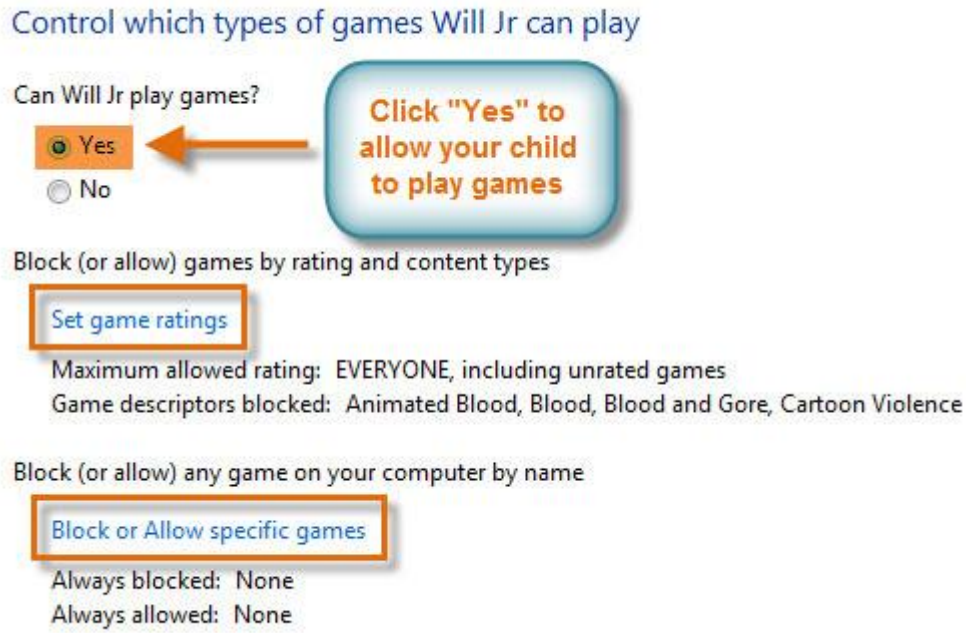


٦. كلیك لەسەر سنووردانی كات Time Limiting دەكەین، بۆ دیاری كردنی كاتی بەكارهێنانی ئەم ئەژمارە و بە پێچەوانەوە لە دەرەوەی سنووری ئەو كاتەی ڕێگەی پێدەدەین ئەژمارەكە كار ناكات، كاتێك بە هۆی سەهمی ماوسەكەوە كلیك لەسەر ئەو خانانە دەكەین كە نامانەوێت لەو ڕۆژ و كاتەدا ئەژمارەكە كار بكات و، ئەو كات و ڕۆژانەش كە دەمانەوێت كاربكات كلیكی لەسەر ناكەین، واتە ڕەنگی شین ڕیگەپێنەدراوە

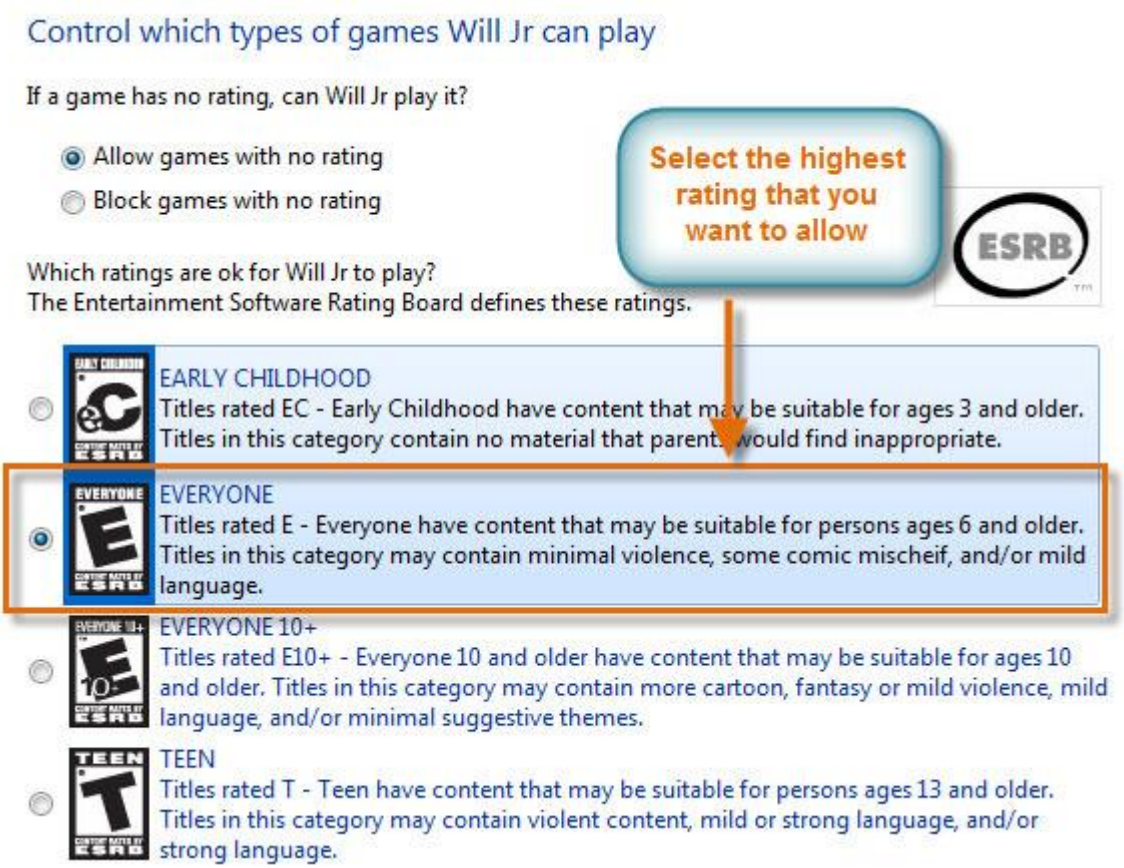


٧. یاری Games، بۆ سنووردار كردنی یاری لە ڕووكارەكەی خاڵی ٥دا، كلیك لەسەر یارییەكان Games دەكەین، پاشان ئەگەر ئەتەوێت ڕێگە بە بەكارهێنەر بدەیت بۆ یاری كردن ئەوا كلیك لەسەر دووگمەی ڕادیۆیی بەڵێ Yes دەكەین و، پاشان بە گوێرەی ژمارەی یاری كردنەكان Set

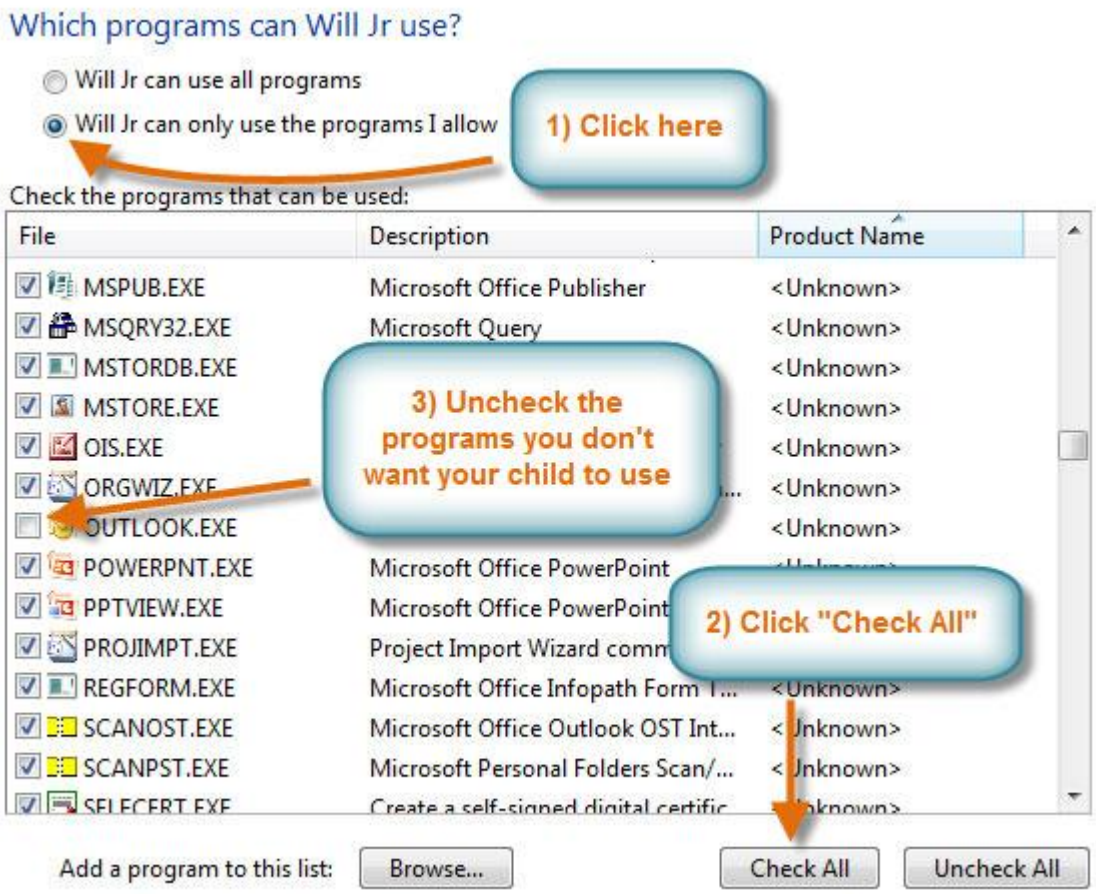
Game Rating ، ڕێگە بەیاری کردن دەدەین یان ڕێگری دەکەین، یاخوود ڕێگە بە یاری دیاری کراو دەدەین یان ڕێگری لێدەکەین Block or Allow Specific Game.



پاشان:



٨. بۆ ڕێگەدان یان ڕێگە گرتن لە بەرنامە، کلیك لەسەر ڕێگەدان ڕێگە گرتن لە یاری یەکی دیاری کراو Allow or Block Specific Software دەکەین لە خاڵی ٥، پاشان کلیك لەسەر Check All دەکەین و، دووانر هەر بەرنامەیەك کە بمانەوێت ئەم بەکارهێنەر نەتوانیت بەکاری بهێنێت کلیکی لەسەر دەکەین و سەحەکەی لادەبەین:

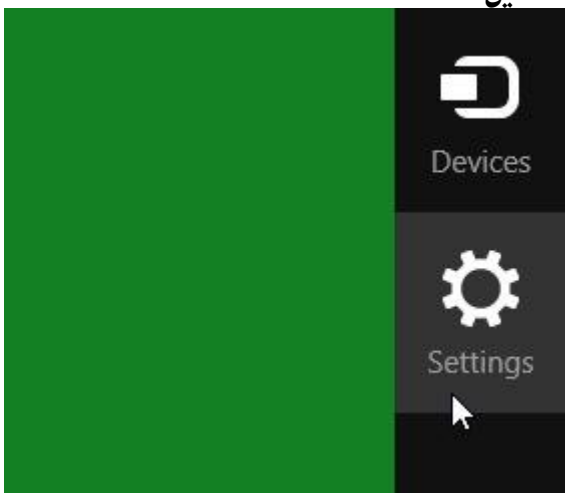


تێپەڕە وشە لە ویندۆز ٨ دا

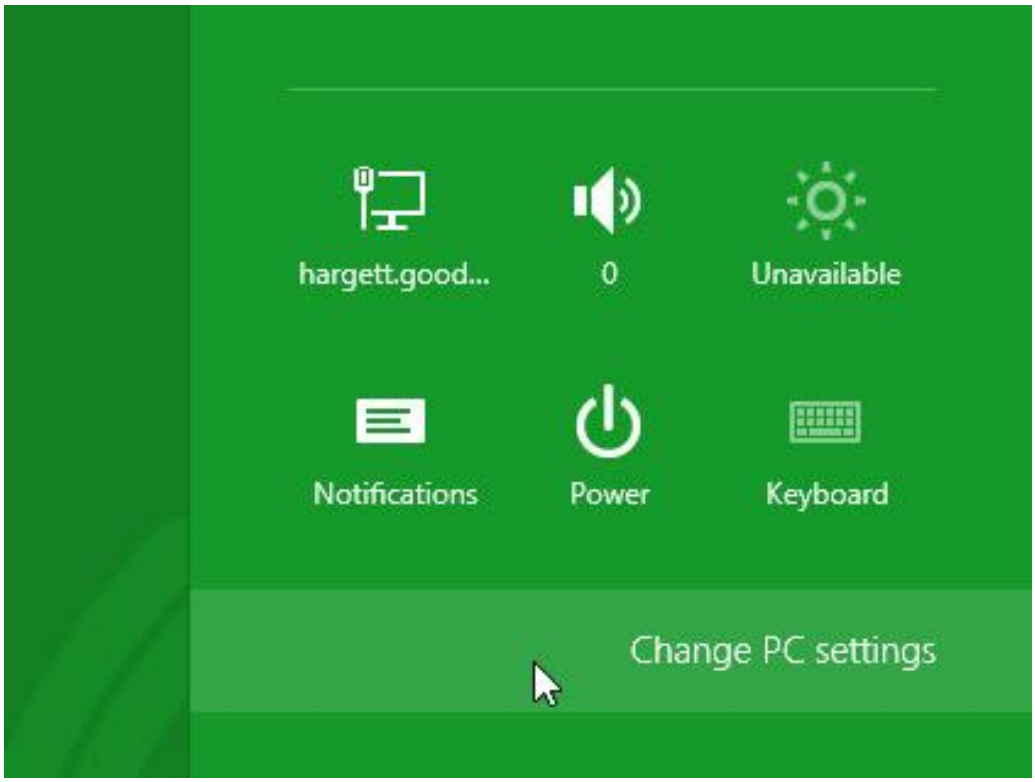
Password in Windows 8

لە ویندۆز هەشتدا بە دوو شێوە سوود لە تیپەرە وشە وەردەگیرێت، بۆ پاراستنی داغڵبوون و داغڵنەبوون، ئەویش لە ڕێگەی ئەژماری مایکرۆسۆفتەوە Microsoft Account، کە ئۆن لاینە، یاخوود لە ڕێگەی ئەژماریی ناوچەییەوە Local Account، بەڵام ئێمە لێرەدا تەنها جۆری دووەم باسەکەین.

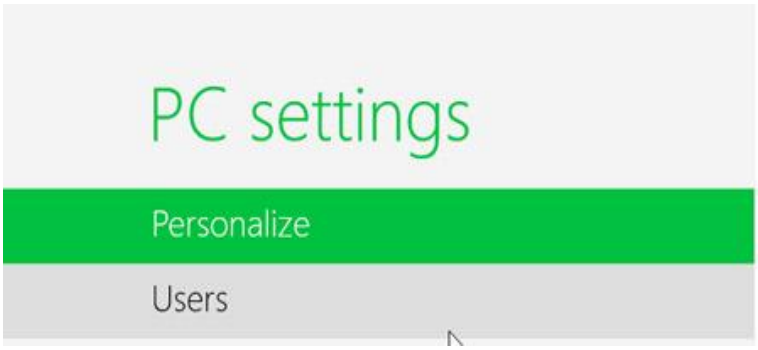
١. کلیك لەسەر ڕێکخستن Settingدەکەین.



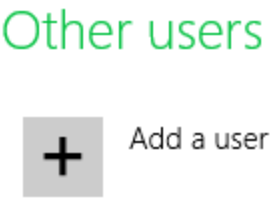
٢. پاشان کلیك لەسەر ڕێکخستنی پی سی PC Settingدەکەین.



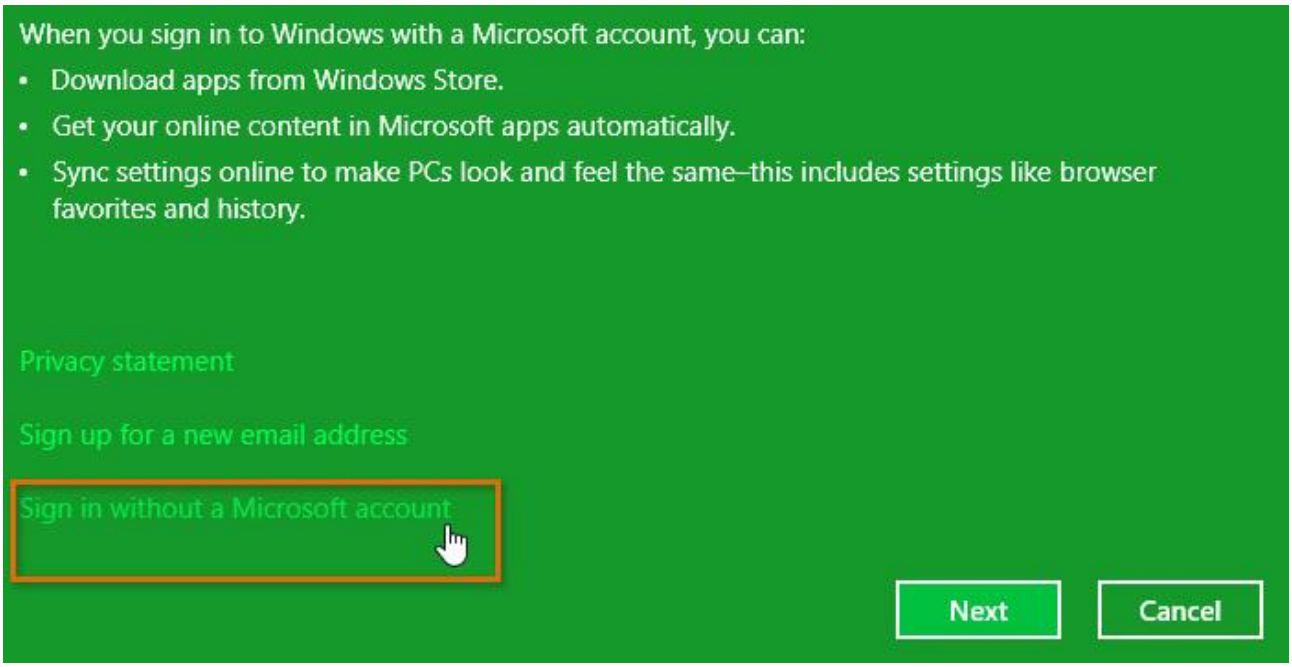
٣. ڕێکخستنی کۆمپیوتەری کەسی PC Settingدەکرێتەوە و، لە لای دەستە چەپ کلیك لەسەر بەکارهێنەرەکان دەکەین:



٤. بەشی بەکارهێنەرەکان دەکرێتەوە Users Paneو، کلیك لەسەر زیاد کردنی بەکارهێنەر Add a User دەکەین:

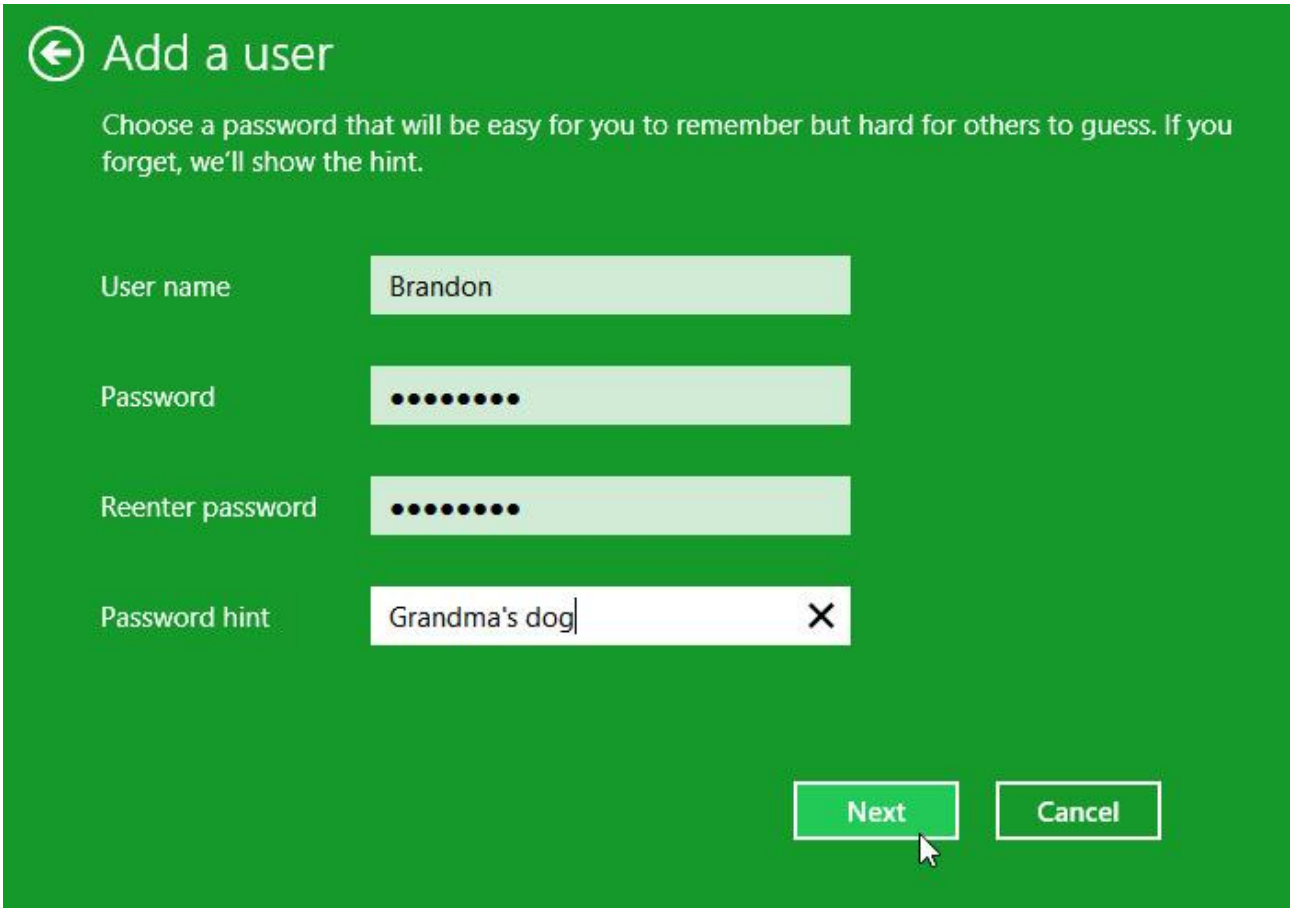


٥. کلیك لەسەر داغڵبوون بەبێ ئەژماری مایکرۆسۆفت Sign in without Microsoft Accountدەکەین:



٦. کلیك لەسەر ئەژماری ناوچەیی Local Accountدەکەین:

٧. روکاری تایبەت بە نووسینی ناوی بەکاربەر و تیپەرە وشە و دووبارە کردنەوەی تیپەرە وشە و بیر خەرەوە دەکریتەوە و پری بکەرەوە و پاشان کلیك لەسەر دوواتر Nextبکە.



٨. پاشان کلیك لەسەر کۆتایی و تەواوبوون Finishبکە و بەمەش کارەکە تەاو بوو .

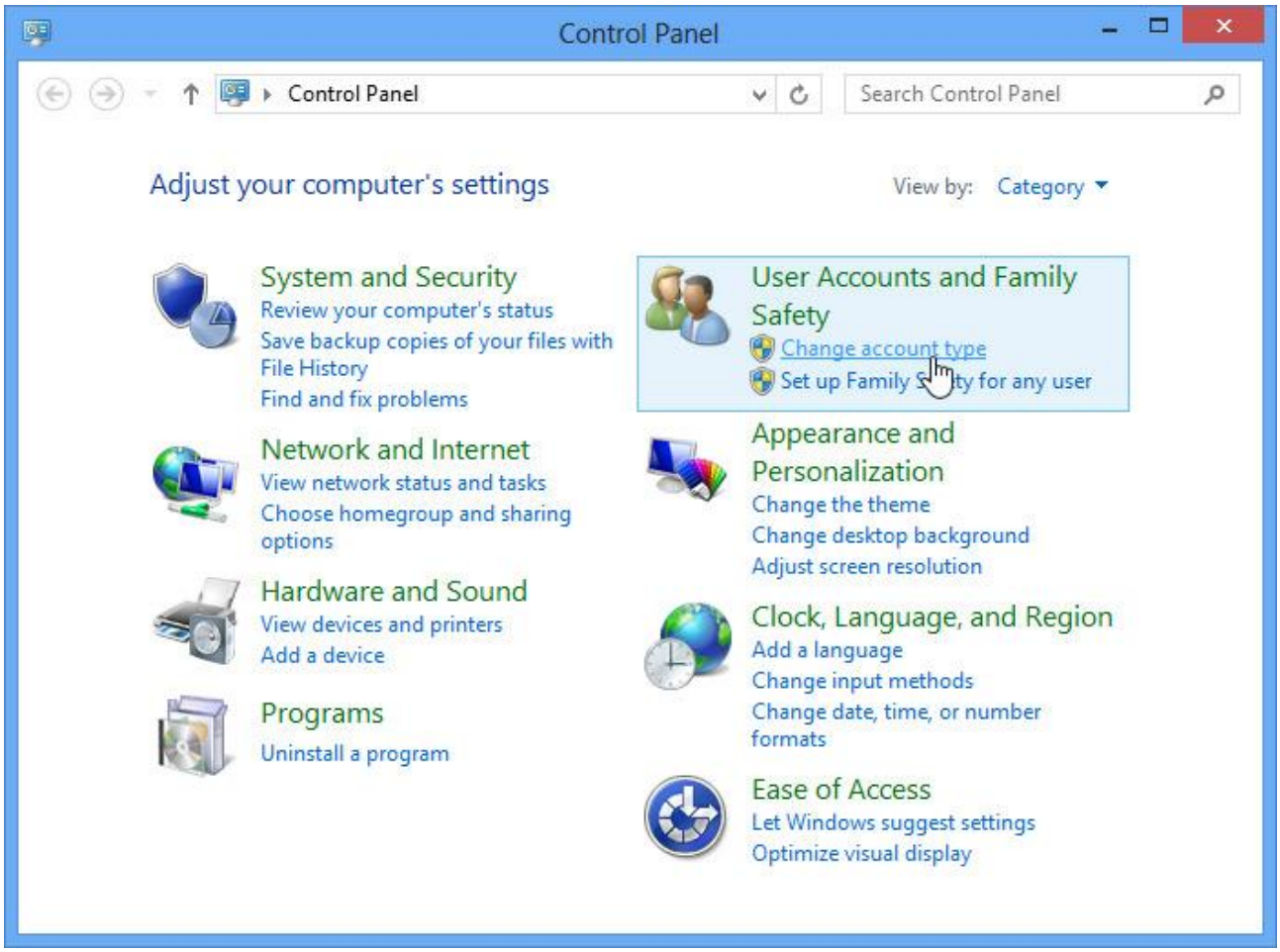
گۆڕینی جۆری ئەژمار و دانانی کۆنترۆڵی باوان

Change User Acount Type & Parental Control

یەکەم//گۆڕینی جۆری ئەژماری بەکارهێنەر:

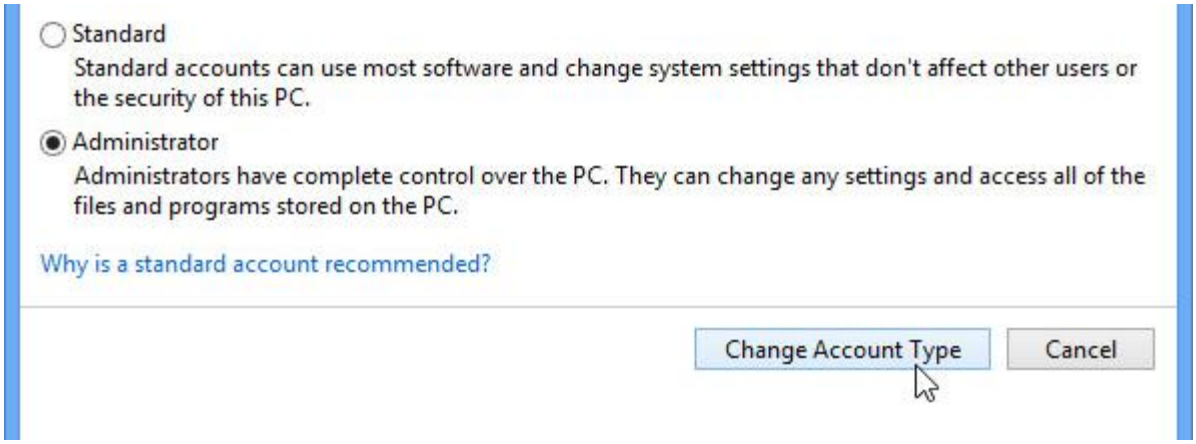
١. پەنیڵی دەستبەسەرا گرتن control Panel دەکەینەوە.

٢. کلیك لەسەر گۆڕینی جۆری ئەژمار Change Account Typeدەکەین.



٣. بەشی تایبەت بە بەڕیوەبردنی ئەژمارەکان دەکرێتەوە Manage Accounts Dialog Box و، کام ئەژمارەی دەتەوێت جۆرەکەی بگۆڕیت کلیکی لەسەر بکە.

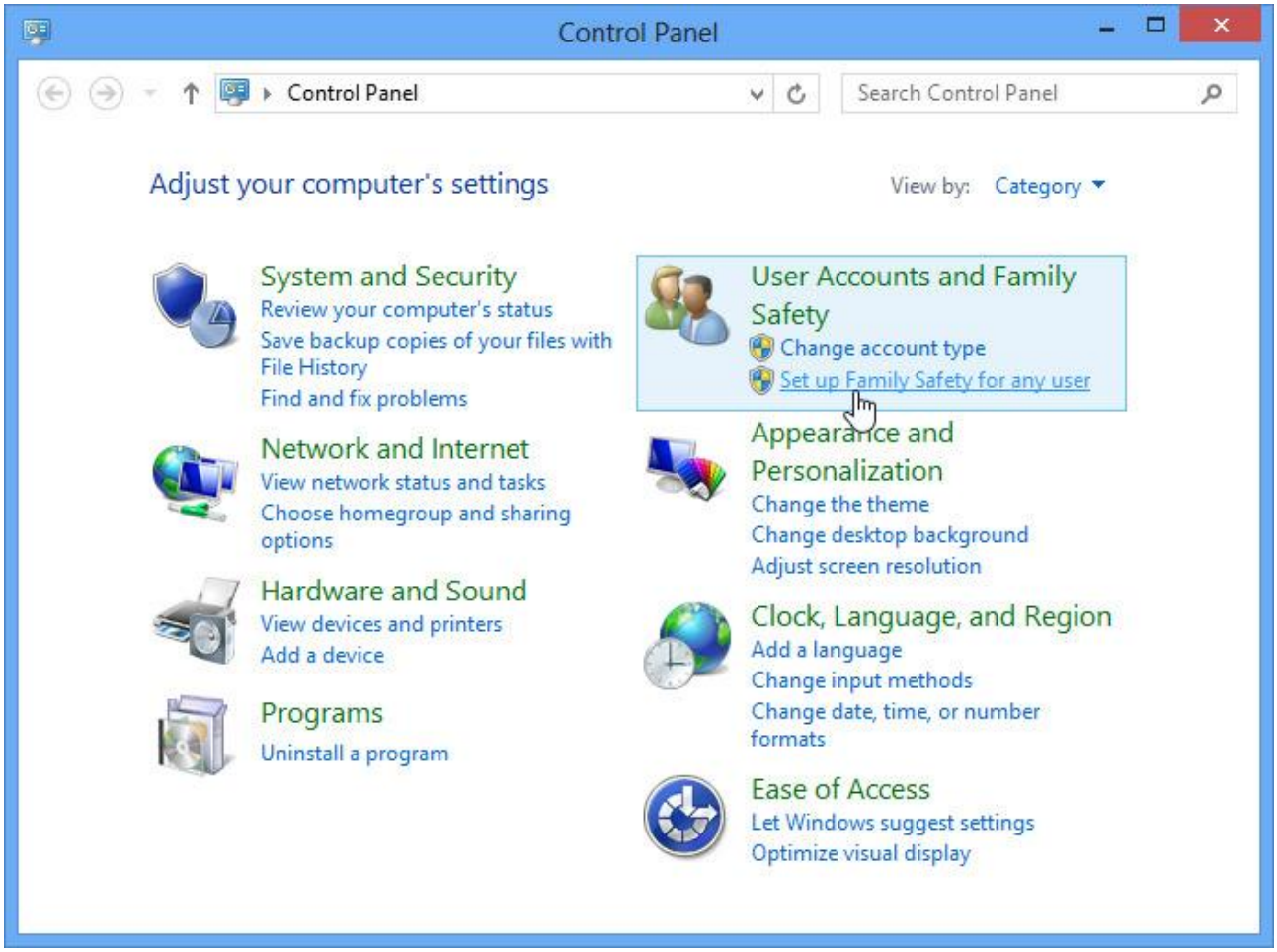
٤. کلیك لەسەر جۆری پێوانەیی Standard بکە و، پاشان کلیك لەسەر گۆڕینی جۆری ئەژمار Change Account Type دەکەین.



دووەم//دانانی کۆنترۆڵی باوان:

١. پەنێڵی دەست بەسەراگرتن Control Panel دەکەینەوە.

٢. کلیك لەسەر دانانی سەلامەتی خێزانی بۆهەر بەکارهێنەرێك Set up Family Sefty for Any User، دەکەین.

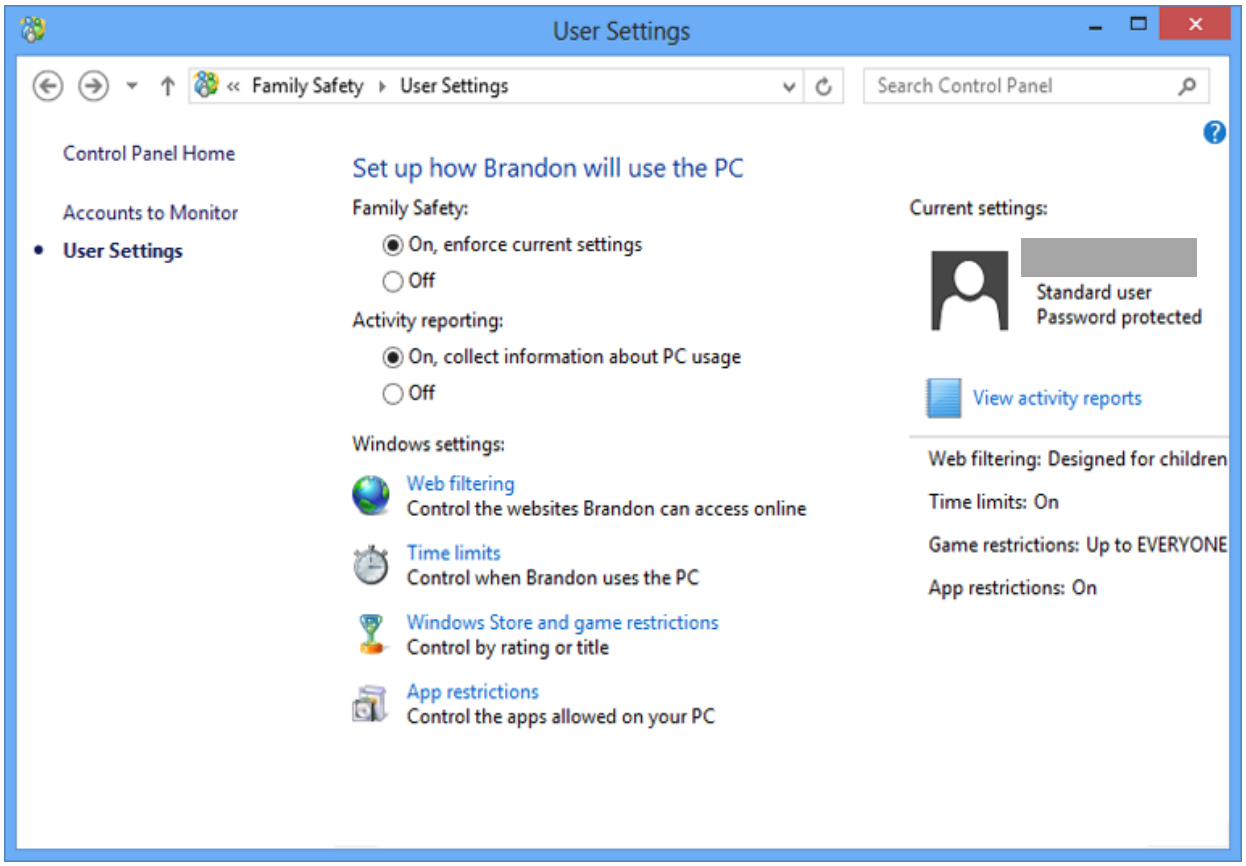


٣. کلیك لەسەر هەر بەکارهێنەرێك دەکەین کە دەمانەوێت کۆنترۆڵی باوانی Parental Control بۆ

دابنێین. بەلام پێویستە ئەژمارەکە لە جۆری پێوانەیی Standard بێت.

٤. بەشی تایبەت بە رێکخستنەکانی بەکارهێنەر User Setting دەکرێتەوە و، بەهۆیەوە دەتوانین سنووربەندی دیاری بکەین:

- بەکلیك کردن لەسەر On ی سەلامەتی خێزان Family Sefty ، بەشەکە چالاك دەکەین.
- راپۆرتی چالاکی Activity Reporting: بە کارپێکردنی ئەم بەشە On دەتوانین راپۆرتی هەفتانە ببینین لە بارەی کات بەسەر بردن و چۆنێتی بەکارهێنانی ئەژمارەکەوە.
- پالاوتنی وێب Web Filtering: بەکاردێت بۆ دیاری کردن و پالاوتنی وێب و، بەهۆیەوە دەتوانین تەنها رێگە بەو سایتانە بدەین کە دەمانەوێت بکرێتەوە Allow List Only، یان نەخشەشازی کراوە بۆ منال Designed For Childern هەلبژێرین.
- سنووردان و کات پێدان Time Limits هەروەك ویندۆز ۷ وایە.
- یاری Gmes یەکان، وەك ویندۆز ۷ وایە.
- بەرنامە App وەك ویندۆز حەوت وایە.
- پیشاندانی راپۆرتی چالاکی View Activity Report: بۆ پیشاندانی راپۆرتی چالاکی هەفتانەی چۆنێتی بەکارهێنانی ئەژمارەکە.



بەشی دووەم

مالْوێر

Malware

مالّـوێـر – Malware

مالّوێر Malware لە هەردوو وشەی Malicious Software وەرگیراوە و، بریتییە لەو زاراوەیەی کە هەموو جۆرەکانی بەرنامە پیس و زیانبەخشەکان دەگرێتەوە و، هەموویان لە ژێر ئەم ناوەدا جێگەیان دەبێتەوە، وەکو ڤایرۆسەکان Viruses، کرمەکان Worms و ئەسپی تەرِوادە Trojan Horses.

هەموو یان بەشێوە و رێگەی جیاواز کاردەکەن و، بچووکن و، خزمەتگوزاری پێشکەش ناکەن و زنجیرەیی نین، بەڵام هەموویان دەتوانن کۆمپیوتەر تووشبکەن Infect و گەندەڵی بکەن Corrupt. دەتوانرێت دابەزێنرێت و بێتە ناو کۆمپیوتەرەوە لە رێگەی ئیمەیڵەوە E-Mail، یان فایلەوە File، لە ئینتەرنێتەوە، هەروەها دەتوانن بڵاو ببنەوە و دابەش ببن بەهۆی تۆڕەکانەوە Networks.

بەشێوەیەکی گشتی بەکاردێت بۆ سازشکردنی کارەکانی کۆمپیوتەر،دزینی زانیاری، تێپەراندنی دەستبەسەراگرتنی دەستپێگەیشتن. یان بە پێچەوانەوە دەبێتە هۆی مەترسی بۆ کۆمپیوتەری خانەخوێ. مالّوێر زاراوەیەکی زۆر باو و بلاوە و، بەکاردێت بۆ جۆرەجیاوازەکانی بەرنامەی زیان بەخش و خراپ، گرنگترینیان بەوردی دەخەینەروو، بەلام جۆرەکانی تریان بە کورتی باس دەکەین.

بێگومان مالّوێرەکان جۆریان زۆرە و، لێرە دا چەند جۆرێکیان باس دەکەین و، ڕوونیان دەکەینەوە و، نمونەی کرداربیان بۆ دەهێنینەوە:

یەکەم// ڤایرۆسەکان Viruses:

ڤایرۆسەکان دروست دەکرێن بە بەکارهێنانی بەرنامەکانی کۆمپیوتەر لەلایەن مرۆڤەکانەوە، پێیان دەوترێت ڤایرۆس لەبەر ئەوەی کۆمپیوتەر تووش دەکەن Infect و گرفتی بۆ دروست دەکەن، ڤایرۆسەکان لەوانەیە زۆر کاریگەربیان هەبێت Effect، هەندێك لەوانە کاریگەربیان کەمە و، هەندێکیان ناوەندە و، هەندێکیان کاریگەربیان زۆر زۆرە و ، ویرانکەر و تێکدەرن.

هەموویان بێزراو و نەویستراون و، لەشێوەی جیاوازدا کاریگەربیان دەردەکەوێت، وەکو تێکدان و خراپ کردنی

فایلی زانیاری، یان دەرکەوتنی لە شێوەی نامە و پەیام دا.

دەتوانین ڤایرۆسی کۆمپیوتەر بەوە پێناسە بکەین کە، بەرنامەیەکی بچوکە، یان بەشێکە لە کۆد ، کە خۆی هاوپێچ Attach ی بەرنامەی تر دەکات و، بڵاو دەبێتەوە کاتێك بەرنامەی خانە خوێ و هەڵگر Host Program لەبەری دەگیرێتەوە Copied، لەلایەن بەکارهێنەرەوە، بۆ کۆمپیوتەرێکی تر، یان دادەبەزێتە ناو ئامێری کۆمپیوتەر لە ڕێگەی تۆڕەکانی ئینتەرنێتەوە کاتێك بەرنامەی خانەخوێ Host Program و هەڵگر، دادەنرێت لەناو تۆڕەکان Networksدا. بەڵام بەزۆری بەهۆی فلاش و دیڤیدی و ..... ،دەگوێزرێتەوە لە ئامێرێکەوە بۆ ئامێرێکی تر، بەهۆی گواستنەوەی فایل و زانیاری خانە خوێ و، هەڵگر و، تووشبووەوە، و زۆر جار زانیاریمان لەسەری نییە. ئەم بەرنامەیە بە کلیك کردن لەسەری چالاك دەبێ و، لەوانەیە کۆمپیوتەرێکیشەوە بگوزرێتەوە بۆ کۆمپیوتەرێکی تر. یان لە فایلێکی هەمان کۆمپیوتەرەوە بۆ فایلەکانی تر.

هەر فایلێك یان بەرنامەیەکی کۆمپیوتەر گونجاوە بۆ ئەوەی ڤایرۆس لێی بدات و، زیانی پێبگەیەنێت، زۆر جار بەهەڵە ئەم وشەیە (ڤایرۆس) بۆهەموو جۆرەکانی مالۆێر Malware بەکاردێت، وەکو کرمەکانی کۆمپیوتەر Computer Worms، ئەسپی تەروادە Trojan Hours، بەرنامەی جاسوس Spy ware، Adware و Rootkits .

زیانەکانی ڤایرۆس

١- خاوکردنەوەی کۆمپیوتەر (توانای وەلاّم دانەوەی کەمدەبێتەوەو، جێبەجێبوونی بەرنامەکانیش خاودەبێتەوە).
٢- لەناوبردنی هەندێك فایل و فولّدەر و، هەندێك جار فایلی بەرنامەکانیش.
٣- هەندێك جار پارچەکانی کۆمپیوتەر تێك دەشکێنێ و لەناویان دەبات، یان دەیان سوتێنێت.
٤- تێکدانی وێنە و نووسین.
٥- تێکدانی بەرنامەکانی کۆمپیوتەر.

خۆپاراستن لە ڤایرۆس

١- وەرگرتنی بەرنامە و فایل و ڤیدیۆ و دەنگ، لە مالّپەڕە (سایتە) باوەرپێکراو و، ناسراوەکانەوە.
٢- سەردان نەکردنی ئەو مالّپەڕانەی جێگەی گومانن (وەك مالّپەڕە سێکسییەکان و .....).

٣- دابەزاندنی جۆرەکانی ئینتەرنێت فێرووێل Internet Firewall.

٤- نەکردنەوەی ئیمەڵە گوماناوی و نەناسراوەکان و، داونلۆد نەکردنی فایلە نەناسراو و گوماناوییە هاوپێچەکان، کە لەگەڵ ئیمەیڵ دا هاتوون.

٥- دابەزاندنی یەکێك لە دژە ڤایرۆسە Anti-Virus بەهێزەکانی وەك (کاسپەر سکای ، نۆرتن ئەنتی ڤایرۆس، نۆدی ٣٢، یان هەر جۆرێکی تر.

-زانین و بڕیاردان لە بارەی جۆری ئەو دژە ڤایرۆسەی بەکاری دەهێنیت.

-زانین لەبارەی هەڵبژاردنەکانەوە کاتێك دژە ڤایرۆسەکە، ڤایرۆس دەدۆزێتەوە و، دەیگرێت. وەکو لابردن Remove، سرینەوە Delete و ..... .

-بەشێوەیەکی رێك و پێك و ماوە ماوە دژە ڤایرۆسەکە نوێبکرێتەوە Update، بە جۆرێك کە هەمیشە نوێترین Newest نوێکراوە Updated وەربگریت.

-دڵنیابوون لەوە ی کە بەرنامەی دژە ڤایرۆسەکە، هەموو ئەو ئامێر و یەکانە ((فلاش میمۆری، دیڤیدی و ....)) بپشکنێت پێش ئەوەی بەکاریان بهێنین و بیانکەینەوە.

-دڵنیتابوونەوە بە پشکینینی هەموو ئەو فایلانی کە لە ئینتەرنێتەوە دای دەبەزێنیت Downloaded بۆ ناو کۆمپیوتەرەکەت.

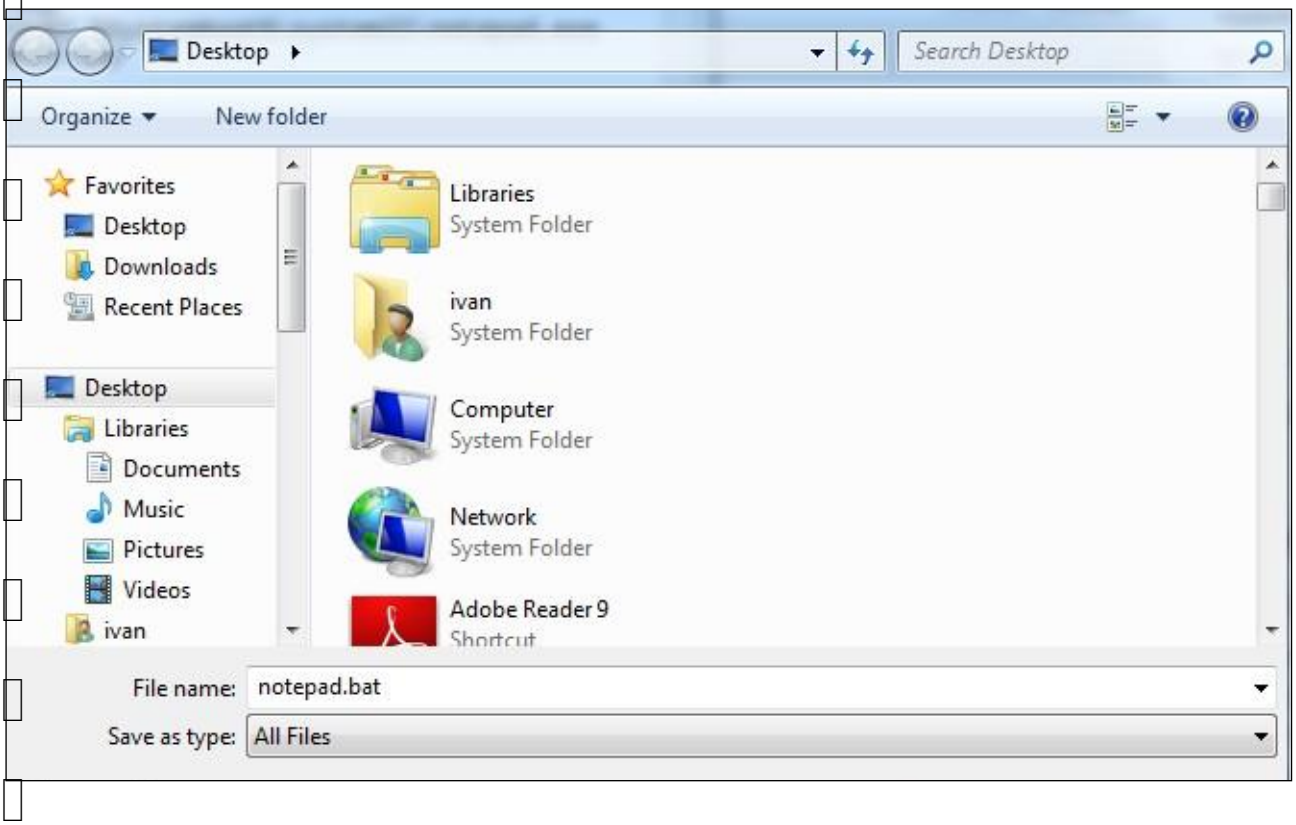
دروست کردنی ڤایرۆسی بێزیان

بۆ کردنەوەی نۆت پاد یان هەر بەرنامەیەکی تر

٢- بەرنامەی نۆت پاد Note Pad بکەرەوە و، ئەم کۆدەی خوارەوە بنووسە :

```
@ECHO off
:top
START %SystemRoot%\system32\notepad.exe
GOTO top
```

٢-فایلەکە پاشەکەوت Save بکە، بە پاشگری (دۆت بات .bat)، بۆنمونە notepad.bat :



تێبینی: کۆدی ئەم ڤایرۆسە تەنها بۆ مەبەستی فێرکردن و تاقیکردنەوەیە، تا زیاتر لە ڤایرۆس تێبگەن و، ئیمە بەرپرسیار نین لە خراپ بەکارهێنانی و، هیوادارم بە خراپ بەکاری نەهێنن.

دروست کردنی سادەترین ڤایرۆس

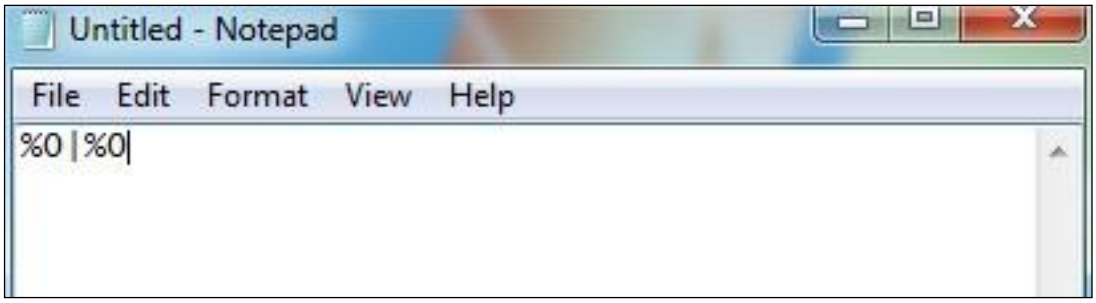
فۆرك بۆمب

Fork Bomb

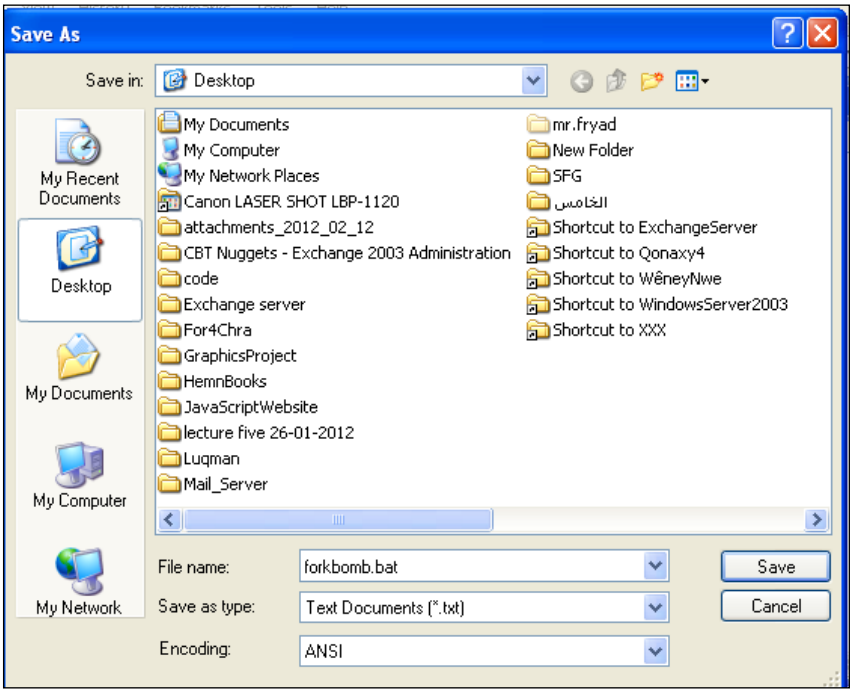
بەهۆی ڤایرۆسی فۆرك بۆمبەوە، بەشێوەیەکی گشتی (یەکەی چارەسەر کردنی ناوەندی – CPU) جامدەبێت (دەوەستێت). بەهۆی کردنەوەی ٥٠٠ پرۆسەی کۆماند پرۆمپت Command Prompt، ئەمەش زەختێکی زۆر دەخاتە سەر CPU و کۆمپیوتەرەکە دەوەستێت.

٣- بەرنامەی نۆت پاد بکەرەوە و ئەم کۆدەی تێدا بنووسە:

```
%0|%0
```



٢- بەپاشگری دۆت بات .bat ، بە ناوێکەوە خەزنی بکە، بۆنمونە forkbomb.bat:



٣-ئێستا بۆمبەکەت دروست کرد و، کرداری (دەستپێکردنەوە بەکار – Restart) بۆ کۆمپیوتەرەکەت ئەنجامبدە، بۆ ئەوەی کارەکە تەواو سەرکەوتوو بێت و، جێبەجێببێت.

تێبینی: کۆدی ئەم ڤایرۆسە تەنها بۆ مەبەستی فێرکردن و تاقیکردنەوەیە، تا زیاتر لە ڤایرۆس تێبگەن و، ئیمە بەرپرسیار نین لە خراپ بەکارهێنانی و، هیوادارم بە خراپ بەکاری نەهێنن.

دروست کردنی ڤایرۆسێك

كه ١٠٠٠ فولّدەر دروست دەكات له چەند چركەیەك دا

ئەم ڤایرۆسە سادە و ساكارە، بەهۆیەوە بێ ئەژمار فولّدەر دروست دەكرێت لەهەر شوێنێكدا، كە بمانەوێ، وەدەتوانین وێنەیەكی جوانی بۆ دابنێین و، بە ناوێكی سەرنج ڕاكێشەوە خەزنی بكەین و، بینێرین بۆ هەر كەسێك كەبمانەوێ، كە بەهۆیەوە تارادەیەك بێزار دەبێت و، هەست بە ڕووداوێكی لەناكاو و، چاوەڕوان نەكراو دەكات.

هەنگاوی یەكەم:

بەرنامەی نۆت پاد بكەرەوە و، ئەم كۆدەی تێدا بنووسە:

```
@echo off
:top
md %random%
goto top
```

شیكردنەوەی كۆدەكە:

دێڕی یەكەم: ئەوە دروست دەكات كە دەربكەوێت لە شاشەیەكی بەتاڵدا.

دێڕی دووەم:

تەنها ناونیشانێكە Label.

دێڕی سێهەم:

ئەم كۆماندە بەكاردێت بۆ دروست كردنی فولّدەرەكان، كە بە شێوەیەكی (عەشوائی – Randomly**) ناو لە فولّدەرەكان دەنێت.**

دیڕی کۆتایی:

گەڕانەوەیە بۆ لەیبڵی تۆپ و، لووپ کردنی بێ پایان ((نا کۆتا)) Infinite loop.

هەنگاوی دووەم:

بەناوێکەوەو، با پاشگری بات bat. **پاشەکەوتی بکە،وەکو** pleasereadme.bat .

هەنگاوی سێهەم:

ئەگەر ویستت خۆت دەتوانیت وێنەیەکی وەکو ئایکۆن بۆ دابنێیت، یان ناوەکەی بگۆڕیت، یان ..... **، بە ئیمەیڵ بینێریت بۆ ئەو کەسەی مەبەستتە بێزاری بکەیت، یان** ..... .

تێبینی: کۆدی ئەم ڤایرۆسە تەنها بۆ مەبەستی فێرکردن و تاقیکردنەوەیە، تا زیاتر لە ڤایرۆس تێبگەن و، ئیمە بەرپرسیار نین لە خراپ بەکارهێنانی و، هیوادارم بە خراپ بەکاری نەهێنن.

لیستی هەندێك لە ڤایرۆسەکان

List of Viruses

Virus	Alias(es)	Types	Subtype	Notes
1260	V2Px	MS-DOS	Polymorphic	First virus to use polymorphic encryption
4K	4096	MS-DOS		The first virus to use stealth
5lo		MS-DOS		Infects .EXE files only

A and A		MS-DOS Windows 95/98		
Abraxas	Abraxas5	MS-DOS Windows 95/98		Infects COM file. Disk directory listing will be set to the system date and time when infection occurred.
Acid	Acid.670, Acid.670a, Avatar.Acid.670, Keeper.Acid.670	MS-DOS Windows 95/98		Infects COM file. Disk directory listing will not be altered.
Acme		DOS (Windows 95MS-DOS)		Upon executing infected EXE, this infects another EXE in current directory by making a hidden COM file with same base name.
ABC	ABC-2378, ABC.2378, ABC.2905	MS-DOS		ABC causes keystrokes on the compromised machine to be repeated.
Actifed		MS-DOS		
Ada		MS-DOS		The Ada virus mainly targets .COM files, specifically COMMAND.COM.
Agena	Agena.723	MS-DOS		Infected programs will have a file length increase of 723 to 738 bytes

AGI-Plan	Month 4-6	MS-DOS		AGI-Plan is notable for reappearing in South Africa in what appeared to be an intentional re-release.
Ah	David-1173, Tuesday	MS-DOS		Systems infected with Ah will experience frequent system hangs.
AI		MS-DOS		
AIDS	AIDSB, Hahaha, Taunt	MS-DOS		AIDS is the first virus known to exploit the MS-DOS "corresponding file" vulnerability.
AIDS II				
AirCop	Air cop-B, Red State	MS-DOS		Infects the boot sector of floppy disks.
Alabama	Alabama.B	MS-DOS		Files infected by Alabama increase in size by 1,560 bytes.
Alcon[1]	RSY, Kendesm, Ken&Desmond, Ether	MS-DOS		Overwrites random information on disk causing damage over time.
Ambulance				
Anna Kournikova		Email VBScript		A Dutch court stated that US$166,000 in damages was caused by the worm.

AntiCMOS				Due a bug in the virus code, the virus fails to erase CMOSinformation as intended.
ARCV-n		MS-DOS		ARCV-n is a term for a large family of viruses written by the ARCV group.
Bomber	CommanderBomber	MS-DOS		Polymorphic virus which infects systems by inserting fragments of its code randomly into executable files.
Brain	Pakistani flu			Considered to be the firstcomputer virus for the PC
Byte Bandit		Amiga, Bootsector virus		It was one of the most feared Amiga viruses until the infamous Lamer Exterminator.
Christmas Tree				
Comm warrior		Symbian Bluetoothworm		Famous for being the first worm to spread via MMS and Bluetooth.
Creeper		TENEX operating system		An experimental self-replicating program which gained access via the ARPANET and copied itself to the remote system.
Eliza		MS-DOS		

Elk Cloner		Apple II		The first virus observed "in the wild"
Graybird	Graybird P			
Hare		MS-DOS Windows 95,Windows 98		Famous for press coverage which blew its destructiveness out of proportion
ILOVE YOU				A computer worm that attacked tens of millions of Windowspersonal computers
INIT 1984		Mac OS		Malicious, triggered on Friday the 13th.
Jeefo				
Jerusalem		DOS		Jerusalem was initially very common and spawned a large number of variants.
Kama Sutra	Blackworm, Nyxem, and Blackmal			Designed to destroy common files such as Microsoft Word, Excel, and PowerPoint documents.
Koko		DOS		The payload of this virus activates on July 29 and February 15 and may erase data on the users hard drive
Lamer Exterminator		Amiga, Boot sector virus		Random encryption, fills random sector with "LAMER"

MacMag	Drew, Bradow, Aldus, Peace			
MDEF	Garfield, Top Cat			
Melissa	Mailissa, Simpsons, Kwyjibo, Kwejeebo	Microsoft Wordmacro virus		Part macro virus and part worm. Melissa, a MS Word-based macro that replicates itself through e-mail.
Michelangelo		MS-DOS		Ran March 6 (Michelangelo's birthday)
Navidad				
Natas		Multipartite, stealth,Polymorphic		
nVIR	MODM, nCAM, nFLU, kOOL, SHIT, prod, Fuck, Hpat, Jude	Mac OS		nVIR has been known to 'hybridize' with different variants of nVIR on the same machine.
OneHalf	Slovak Bomber, Freelove or Explosion-II	MS-DOS		It is also known as one of the first viruses to implement a technique of "patchy infection"

Ontario .1024				
Ontario .2048				
Ontario	SBC	MS-DOS		Death Angel
Pikachu virus				The Pikachu virus is believed to be the first computer virus geared at children.
Ping-pong	Boot, Bouncing Ball, Bouncing Dot, Italian, Italian-A, VeraCruz	Boot sector virus		Harmless to most computers
RavMonE.exe	RJump.A, Rajump, Jisx	Worm		Once distributed in Apple iPods, but a Windows-only virus
SCA		Amiga, Boot sector virus		Puts a message on screen. Harmless except it might destroy a legitimate non-standard boot block.
Scores	Eric, Vult, NASA, San Jose Flu	Mac OS		Designed to attack two specific applications which were never released.
Scott's Valley		MS-DOS		Infected files will contain the seemingly meaningless hex string 5E8BDE909081C63200B912082E.

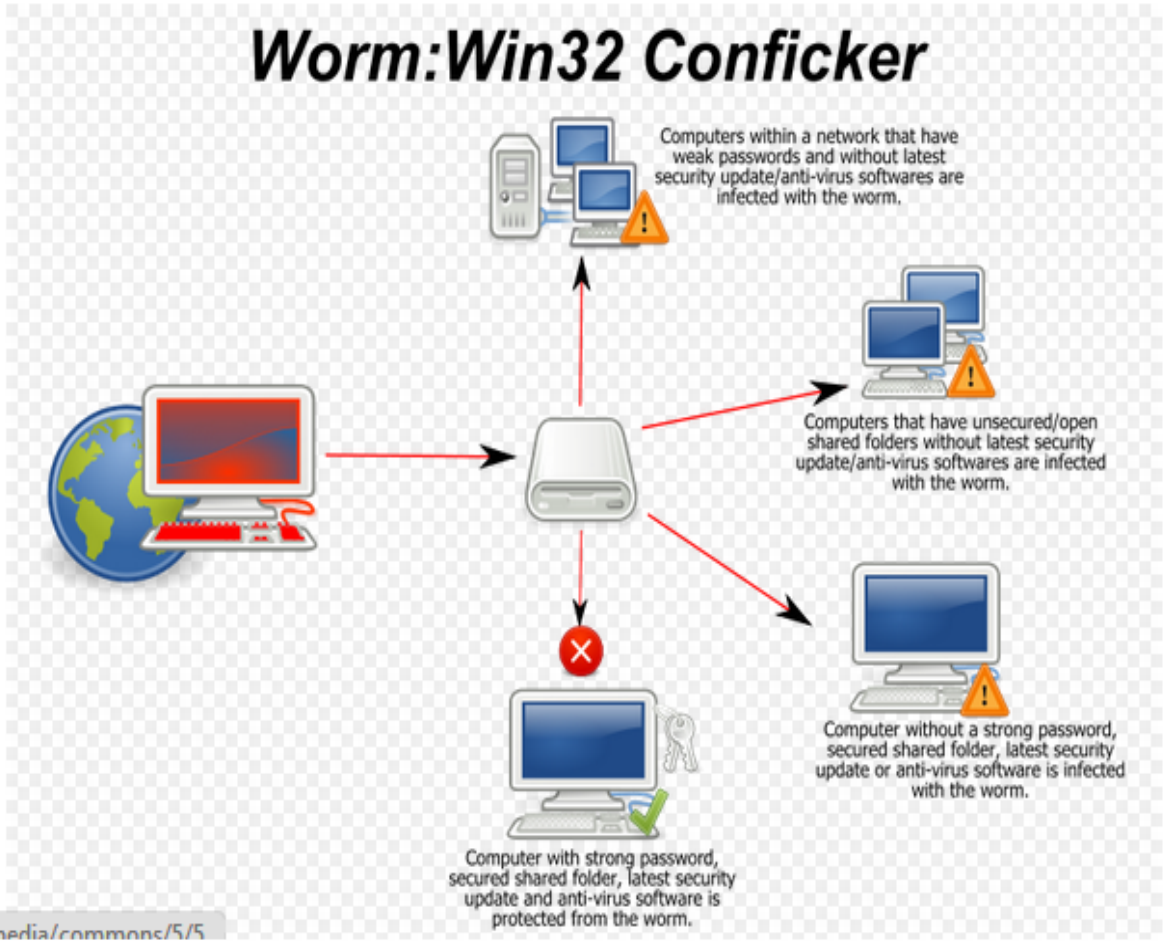
Seven Dust	666, MDEF, 9806, Graphics Accelerator, SevenD	Mac OS		
Shankar's Virus	W97M.Marker.o	PolymorphicVirus		Infects Word Documents
Shoerec		Windows 32		
Simile	Etap, MetaPHOR	Windows	Polymorphic	The metamorphic code accounts for around 90% of the virus' code
Stoned				One of the earliest and most prevalent boot sector viruses
Sunday		MS-DOS	Jerusalem.Sunday	Because of an error in coding, the virus fails to execute its payload.
TDL-4		Botnet		
Techno		MS-DOS		The virus plays a tune that was created by the author of the virus
Whale		MS-DOS	Polymorphic	At 9216 bytes, was for its time the largest virus ever discovered.
ZMist	ZMistfall, Zombie.Mistfall	Zombie.Mistfall		It was the first virus to use a technique known as "code integration".

دووەم// کرمەکان – Worms

کرمەکان – Worms

جۆرێکی مالویرن،خۆیان کۆپی دەکەن و بەناو تۆرەکاندا بلاودەبنەوە،پێویستیان بەوە نییە هاوپێچ Attach ی بەرنامەی تربن بۆ بلاو بوونەوەیان، هەروەها پێویست ناکات بەکارهێنەر دەست تیوەردان و دەست کێشانە ناوی Intervention هەبێت بۆ بلاوبوونەوە Spreadو پەخشکردنی کرمەکان.

کرمەکان دەبنە هۆی زیان و مەترسی بۆ تۆرەکان (ڕایەڵەکان) Networks، و هەندێکیان هیچ گۆرانێك ناکەن لەو سیستەمەی بەناوی دا، دەڕۆن.



جۆرەکانی کرم

Worm Types

کرمەکان زۆر جۆری جیاوازیان هەیە و، بەشێوەیەکی گشتی لە پێنج جۆری جیاوازدا پۆلێن دەکرێ، بەلام بەردەوام گۆرانکاری ی ڕووەدات و جۆر و شێوەی نوێ دروست دەبێ:

١.کرمەکانی نامەی ئەلیکترۆنی E-Mail Worms

کرمەکانی ئیمەیڵ ئەو کرمانەن کە نامەکان تووش دەکەن، و دەگوێزرێنەوە و دەجوولێن بەهۆی لینکی ئێچ تی ئێم ئێلەوە HTML Link ، یاخوود بە هۆی هاوپێچەکانی نامەوە E-Mail Attachment کە دەنێردرێت، لە لایەن سایتە تووشبووەکانەوە کە کرمیان هەیە و، ئەگەر بەکارهێنەر هاوپێچەکانی نامەکە، یان لینکی ئێچ تی ئێم ئێڵ بکاتەوە، کرمی ئیمەیڵ توانای تووشکردنی سیستەمی کۆمپیوتەری هەیە Computer System.

کرمەکانی ئیمەیڵ دەتوانن بلاوببنەوە بەهۆی بەنامەکانی مایکرۆسۆفت ویندۆزەوە، وەکو کارەکانی ویندۆز ئێم ئەی پی ئای Windows MAPI Functions، یان خزمەتگوزارییەکانی مایکرۆسۆفت ئاوتلووکەوە Microsoft Outlook Services،

کرمەکانی ئیمەیڵ توانای دزین و بەکارهێنانی ناونیشانی ئیمەیڵی بەکارهێنەری هەیە لە دەفتەری ناونیشانەوە Address Bookیان لە سەرچاوەکانی بەرنامەی ترەوە Other Program Sources. بێگوومان تۆمەتبار کردنی هەڵە ڕووەدات کاتێك بەکارهێنەر نازانێت کام لەو نامانەی بۆی هاتووە، نامە تووسبووەکە بووە.

٢.کرمەکانی ئینتەرنێت Internet Worms:

کرمەکانی ئینتەرنێت هەولدەدەن بۆ دۆزینەوەی خاڵی لاواز و نەپارێزراوی سیستەمی کۆمپیوتەر Vulnerable Computer System، بەهۆی پشکنینی تۆرەکانی کۆمپیوتەر بە

بەکارهێنانی سیستەمی کارپێکەری ناوچەیی Local Operating System. دووای ئەوەی کرمەکانی ئینتەرنێت خالێکی پێکەوە بەستنی جێگیریان Stable Connection دۆزییەوە، دەستپێگەیشتنی تەواو بەدەست دەهێنن بۆ سیستەمی کۆمپیوتەر و، بە ئاسانی داغڵی دەبن، کرمەکانی ئینتەرنێت توانا و لێهاتوییان هەیە بۆ دابەزاندنی بەرنامە Install Program و، ناردنی زانیاری بۆ سیستەمی کۆمپیوتەری تووشبوو.

٣.کرمەکانی چاتی وەرگرتن و پیارۆشتن بە ئینتەرنێت دا Internet Relay Chat (IRC) Worms:

کرمەکانی چات ئامانجیان ژوورەکانی چاتە chat room یان ساحەکانی نامە Message Forums، کە بەشێوەیەکی گشتی ناسراوون وەکو ڕێڕەو ((چەناڵ)) ی چات Chat Channel ، بەهۆی ناردنی لینکی سایتێکی توشبووە، یان فایل بۆ بەکارهێنەر، ئەم جۆرەیان کەمتر کاریگەری هەیە لە چاو جۆرەکانی تری کرمی کۆمپیوتەر دا، چونکە وەرگری کرمەکە دەبێت پشت ڕاستی بکاتەوە Confirm، پاشەکەوتی بکات Save و بیکاتەوە Open، بۆ تووشکردنی سیستەمی کۆمپیوتەرەکە.

٤.کرمەکانی نامە و پەیامە هەنووکەییەکان Instant Message Worms:

ئەم کرمانە دەردەکەون لە بەرنامەی نامە و پەیامە هەنووکەییەکان دا Instant Messages Applications، وەکو یاهو مێسنجەر Yahoo ! Messenger، و ناردنی لینکی سایتێکی توشبوو بۆ پەیوەندییەکەت دەکەنە هۆکاری تووشکردنی کۆمپیوتەر، ئەم کارەش وەکو کرمەکانی ئیمەیڵ وایە، بەڵام لیستی پەیوەندی پەیامبەر بەکاردەهێنێت بۆ بڵاوکردنەوەی لینکە تووشبووەکان.

٥.کرمەکانی رایەڵەی بلاوکردنەوەی فایل File – Sharing Network Worms:

ئەم کرمانە خۆیان کۆپی دەکەنەناو Copy فولدەری هاوبەش و بڵاوکراوە Shared Folder و،

تیایدا دەردەکەون وەکو اوێکی بێزیان. یەك فایل دەستدەکات بە بڵاوکردنەوە و تووشکردن بە ناو تۆری بڵاوکردنەوەی فایل File – Sharing Networkدا، ئەم کاری تووش کردنە بەر دەوام دەبێت، هەتاوەکو سیستەمەکانی تریش تووش دەکات.

نیشانەکانی کرمی کۆمپیوتەر

Symptoms of Computer Worm

کاتێك کرمەکان کۆمپیوتەرەکان تووشدەکەن، بە هۆی کۆمەلێك نیشانەی دیار و بەر چاوەوە دەتوانین ئەم تووش بوونە هەست پێبکەین و، دیاری بکەین، بەشێوەیەکی گشتی نیشانەکان ئەمانەی لای خوارەوەن:

١.خاو کردنەوەی جیبەجێکردنی کۆمپیوتەر Computer Performance.

٢.لە جولەخستن و وەستان لە نرخێکدا Freezingو هەرەسهێنان و تیکشکانێکی کوتوپڕ و لەناکاو Crashing.

٣.کرانەوە و جیبەجێکردنی بەرنامە بەشێوەیەکی خۆکاری و ئۆتۆماتیکی.

٤.ناڕێك و پێکی لە جێبەجێکردن و کارکردنی وێبگەڕ Web Browser رووەدات.

٥.هەلسووکەوت و رەفتار نا ئاسایی دەبینرێت وەکو نامە، وێنە،دەنگ و .... .

٦.ئاگادارکردنەوەی دیواری ئاگرین Firewall دەبینرێت.

٧.لە دەستچوون و گۆڕانکاری بچووك لە فایلدا رووەدات.

٨.دەرکەوتنی نامە و پەیامی بوونی هەڵە و گرفت لە سیستەم و سیستەمی کارپێکردن Operating Systemدەردەکەوێت.

۹.نامەی نیردراو بۆ پەیوەندییەکانت بەبئ ئەوەی زانیاری لەسەر نیرەرەکەی زانراو و بەردەست بێت.

لیستی کرمەکان

List of Worms

لەم لیستەی خوارەوەدا، هەندیك كرم و زانیاری لەبارەیانەوە خراوەتە روو، تەنها بۆ مەبەستی وەرگرتنی زانیاری لە سەر کرمەکانی کۆمپیوتەر ئەم لیستە دروست کراوە:

Name	Alias(es)	Isolation	Author	Notes
Badtrans				Installed akeylogger; distributed logged information
Bagle	Beagle, Mitglieder, Lodeight	Mass mailer		
Blaster	Lovesan	Gruel.exe Makes all exe's unusable so the computer probably can't reboot	Jeffrey Lee Parson	Targeted toward Bill Gates; contained message "billy gates why do you make this possible ? Stop making money and fix your software!!"
Brontok	W32/Rontokbro.gen@MM, W32.Rontokbro@mm, BackDoor.Generic.1138, W32/Korbo-B, Worm/Brontok.a, Win32.Brontok.A@mm, Worm.Mytob.GH, W32/Brontok.C.worm, and Win32/Brontok.E, W32.Rontokbro.D@mm.			Spread through an Indonesian e-mail headed with "stop the collapse in this country"; destroys firewalls
BuluBebek	W32/VBWorm.QXE			
Code Red	ndjupi			This worm allows the hackers to hack your complete network
Daprosy Worm	Worm.Win32.VB.arz, W32.Autorun.worm.h, W32/Autorun-AMS, Worm:Win32/Autorun.UD			Replaces folders with .EXE's, key logger, slow mass mailer

Code Red II				Exploited MicrosoftInternet Information Server security holes.
Dabber	W32/Dabber-C, W32/Dabber.A			
Doomjuice				Attacked computers that had previously been infected by theMydoom worm.
ExploreZip	I-Worm.ZippedFiles			Spread through zipped documents in a spam e-mail.
Father Christmas	HI.COM			
Hybris	Snow White, Full Moon, Vecna.22528		Vecna	Spread through an e-mail from "haha@sexyfun.net"
ILOVEYOU	Loveletter, LoveBug			
Kaja	Parasite			
Kak worm				Restarted the computer after 5pm, on the first day of each month, and displayed the message: "Driver Memory Error - Kagou-Anti-Kro$oft says not today !"
Klez				
Koobface				Targeted MySpace and Facebook users with a heading of "Happy Holidays"
Mabutu				
Melissa	Simpsons, Kwyjibo, Kwejeebo		David Smith	Not originally intended as harmful, but crashed servers by flooding them with e-mail
Morris			Robert Tappan Morris	This computer worm has been spread by the hackers,so that they could easily spy your computer without your notification, they can even steal your passwords, Internet banking and personal data. This process is a security risk and should be removed from your system else It will unintentionally slowed and crashed computers.

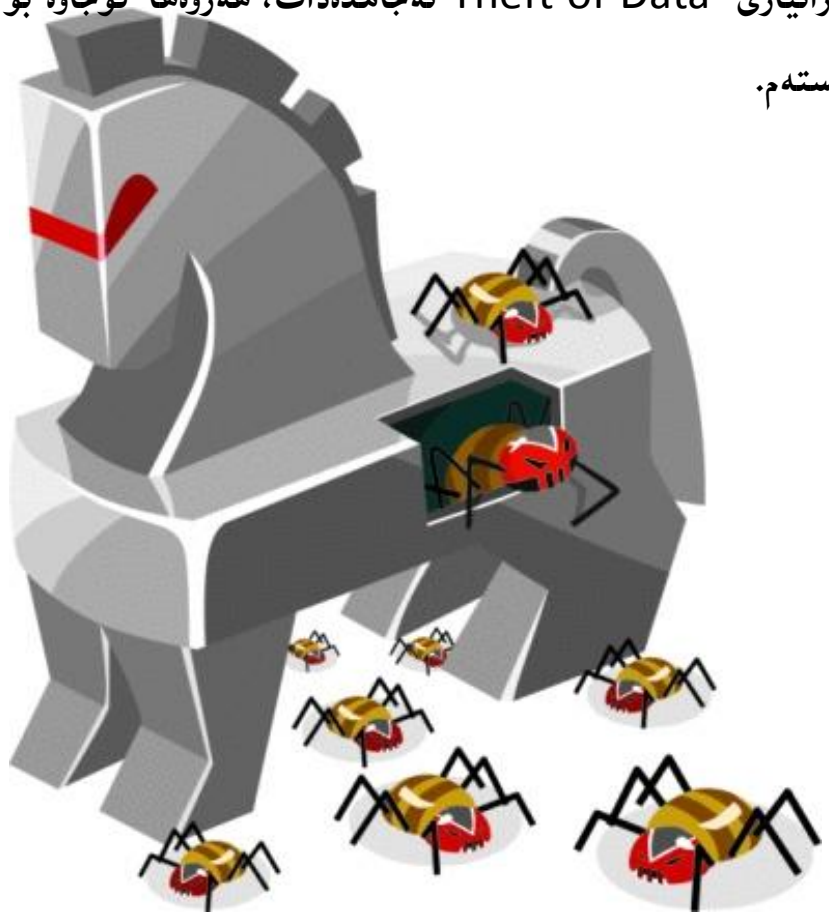
Mydoom	W32.MyDoom@mm, Novarg, Mimail.R, Shimgapi			Fastest-spreadinge-mail worm known; used to attack SCO Group.	
Mylife	W32.MyLife.C@mm			[1]	
Navidad					
Netsky			Sven Jaschan		
Nimda				Originally suspected to be connected toAl Qaeda because of release date; uses multiple infection vectors	
Sadmind					
Sasser	Big One		Sven Jaschan		
Sircam				Spread through e-mail with text like "I send you this file in order to have your advice."	
Sober	CME-681, WORM_SOBER.AG			Was disguised as e-mail from United States government.	
Sobig					
SQL Slammer	DDOS.SQLP1434.A, the Sapphire Worm, SQL_HEL, W32/SQLSlammer			Caused global Internet slowdown	
Stuxnet	Win32/Stuxnet			First malware to attack SCADAsystems.	
Swen					
Supernova Worm	Supova, Hello Kitty			Posed as files relating to video games Quake andGrand Theft Auto; attacked Christian websites	
Upering	Annoyer.B, Sany				

سێیەم: ئەسپی تەروادە

Trojan horse

ئەم ئەسپی تەروادەیە جۆرێکی تری مالۆێرە. بەرنامەیە کە دەردەکەوێت لە شێوەیەکی سوودبەخش Usefulدا، بەڵام کاتێك بەرنامەکە جێبەجێدەکرێت لەگەڵیدا بەرنامەیەکی زیانبەخش و پیس Malicious یان فرمانێك Commandدادەبەزێت Install یان جێبەجێدەبێت لەسەر کۆمپیوتەرەکە، بە بێ ئەوەی بەکارهێنەر زانیاری هەبێت لە بارەیەوە.

بەمانایەکی تر دەتوانین بڵێین بەرنامەیەك دەبێتە هەڵگر و گوێزەرەوەی کۆدێکی خراپ و پیس و زیانبەخش Malicious Code و، کاتێك بەکارهێنەر کارێکی تایبەتی بەو بەرنامەیە هەیە و، بەکاری دەهێنێت و، دایدەبەزێنێت یان بەکاری دەهێنێت ئەوا ئەم کۆدە خراپ و زیانبەخشە چالاك دەبێت و کلۆی خۆاپی خۆی دەکات، کە بەشێوەیەکی گشتی هەردوو کاری فەوتاندنی زانیاری Loss of Data و دزینی زانیاری Theft of Data ئەنجامدەدات، هەروەها گونجاوە بۆ ئەوەی ببێتە زیان و مەترسی بۆ سیستەم.



زاراوە و بیرۆکەی ئەسپی تەروادە Trojan Horse لە چیرۆکی Wooden Horse وەرگیراوە، کە پێشکەش کردنی ئەسپێکی دارینی پڕ لە جەنگاوەری ئازا و دلێر بوو بۆ قەلاکە، وەك دیاریيەکی جوان و باش و سوود بەخش دەهاتە پێش چاو لە رووالەت دا، بەڵام ناو ئەسپەکە جەنگاوەری تێدابوو، خەڵکی قەلاکە نەیانزانی و بردیانە ناو قەلاکە، بەمەش خەڵکی قەلاکە بە رووالەتی ئەسپەکە فریوویان خوارد و، دووژمنەکەیان بە دەستی خۆیان بردە ناو قەلاکەی خۆیان، بەکارهێنەری کۆمپیوتەریش بەهەمان شێوەیە و، ئەسپی تەروادەی کۆمپیوتەر بەە هەمان شێوە کار دەکات.

جۆرەکانی ئەسپی تەروادە

Trojan Horses Types

ئەپسپی تەروادە زۆر جۆری هەیە و، بە چەند شێوەیەکیش پۆلێن کراوە و، یەکێك لەو پۆلێنانە پشت دەبەستێك بە چۆنێتی تێکشکاندنی سیستەم و وێرانکردنی، بەم پێیە چەند جۆرێکی سەرەکی ئەسپی تەروادەمان هەیە، بەم شێوەیە:

١. ترۆجانەکان دەستپێگەیشتن و داغلّبوون لە دوورەوە Remote Access Trojans.

٢. ترۆجانەکانی ناردنی زانیاری Data Sending Trojans یان ناردنی تێپەرە وشە Password Sending.

٣. ترۆجانە تێکشکێنەرەکان Destructive Trojans.

٤. ترۆجانەکانی نوێنەری و جێگری Proxy Trojans.

٥. ترۆجانەکانی (پرۆتۆکۆلی گواستنەوەی فایل) File Transfer Protocol (FTP) Trojans.

٦. ترۆجانە لە کار خەر و زەبوونکەرەکانی بەرنامەی پاراستن Security Software Disabler

.Trojans

۷. ترۆجانەکانی هێرشکرنەسەر پەسەند نەکردنی خزمەتگوزاری Denial – of – Service Attack (DoS) Trojans.

۸. ترۆجانەکانی کوشتن و تێکشکاندنی سیستەم System Killing Trojans

۹.ترۆجانەکانی بۆمبی ئیمەیڵ Mail – Bomb Trojans.

جۆری هەڵگر و گوێزەرەوەکانی ترۆجان

Type of Trojan horse Payloads

هەڵگر و گوێزەرەوەکانی ئەسپی تەروادە، بە شێوەیەکی پۆلێن دەکرێن بۆ دوو جۆری سەرەکی، کە بە کورتی ئاماژەیان پێدەکەین:

یەکەم: بۆمبی لۆژیکی و بۆمبی کات Time Bomb and Logic Bomb.

دووەم: درۆپەرەکان Droppers.

مەبەست و بەکارهێنانەکان

Purpose & Uses

ترۆجان بە زۆری لەلایەن هاکەرزەکانەوە بەکاردەهێنرێت بۆ ئەوەی لە دوورەوە دەستیان بگات بە زانیارییەکان Remote Access بۆ مەبەستێکی دیاری کراو و، دەستگەیشتن بە سیستەمی کۆمپیوتەر، کارەکەش جێبەجێدەکرێت لەلایەن هاکەرزەوە بۆ ئەم مەبەستانەی خوارەوە:

- دزینی پارەی ئەلیکترۆنیکی Electronic Money.
- بەکارهێنانی ئامێر وەکو بەشێك لە بووتنێت Botnet.

- دزینی زانیاری Data Theft.
- گۆرانکاری بچووك یان سرینەوەی فایل.
- دابەزاندن Downloading یان بەرزکردنەوە Uploading ی فایل بۆ مەبەستی جیاواز جۆراو جۆر.
- بینین و تەماشاکردنی شاشەی بەکارهێنەر.
- سەیرکردنی کامێرای ئینتەرنێتی بەکارهێنەر.
- دەست بەسەراگرتنی سیستەمی کۆمپیوتەر لە دوورەوە.
- گۆرینی تۆمارەکان.
- سرینەوەی بەرنامەکان Uninstalling Software.
- بڵاوکردنەوەی جۆرەکانی تری مالۆێر Spread Other Malware.
- بەکارهێنانی کۆمپیوتەری تووشبوو وەکو نوێنەر و بریکار بۆ ئەنجامدانی چالاکی نایاسایی یان هێرشکردنەسەر کۆمپیوتەری تر.
- خراپکەری زانیاری ((گەندەڵی)) Data Corruption.
- فۆرماتی دیسکەکان Formatting Disc و تێکشکاندنی ناوەرۆکەکەی Destroy All Content.
- تیکشکاندێکی کوتوپڕ و لەناکاوی کۆمپیوتەر Crashing the Computer لەگەڵ شاشەی مردن Blue Screen of Death.

بێگومان زۆر مەبەست و بەکارهێنانی دیکەمان هەیە و، لێرەدا تەنها ئەوەندە بە پێویست دەزانین بیانخەینە ڕوو، بۆیە لەوە زیاتر ئاماژە پێناکەین.

ئەسپەتەراوەدە باوەکان

Common Trojan Horses

ژمارەیکی زۆر ئەسپی تەروادەمان هەیە و، ناتوانین هەموویان بهێنینەوەو، بیاننناسێنین بۆیە لێرەدا زۆر بەکورتی و تەنها ترۆجانە باوەکان دەنووسین:

- **PC Optimizer Pro (unknown creator)**
- **Netbus (by Carl-Fredrik Neikter)**
- **Subseven or Sub7(by Mobman)**
- **Back Orifice (Sir Dystic)**
- **Beast**
- **Zeus**
- **Trojan.Agent**
- **The Blackhole exploit kit[12]**
- **Flashback Trojan (Trojan BackDoor.Flashback)**
- **ProRat**
- **ZeroAccess**
- **Koobface**
- **BetterSurf**

چوارەم//بەرنامەکانی جاسوسی

Spy Ware

بەرنامەی جاسوسی Spy Ware جۆرێکی مالۆێرە، کە کاری جاسووسی دەکات لەسەر چالاکییەکانی بەکارهێنەر، توانای ئەم جاسووسی کردنە چاودێری چالاکیی Activity Monitoring، کۆکردنەوەی پەنجەپیانانەکانی کیبۆرد Collect Keystrokeواتە هەر پەنجەنانێك بە هەر دووگمەیەکی کیبۆرد دا وەردەگرێت و، کۆی دەکاتەوە و بەکاری دەهێنێت، هەروەها زانیاری ژمێرەیی، داغڵبوون، زانیاری مالی.

چاودێری و جاسووسی دەکات لەسەر قوربانییەکان، خۆی دەشارێتەوە و بە شاردراوەی دەمێنێتەوە، ئەتوانێت چالاکی جیاواز ئەنجام بدات، مەبەست لەوەیە کە هێرشبەر توانای بینینی تیپەرەوشەی Password قوربانی یەکەی هەیە و، بەهۆیەوە داغڵەبێت بۆ ئەژمارەکەی یان کۆمپیوتەرەکەی .

بەرنامەی جاسووسی Spy Ware بەشێوەیەکی گشتی بەکاردێت بۆ دزینی زانیاری نهێنی و تایبەتی و گرنگ.

جۆرەکانی تری مالّوێر

Other Types of Malware

جۆرە گرنگ و باوەکانی مالّوێرمان بە وردی رووونکردەوە، بەلام جۆرەکانی تر بە کورتی باسیان دەکەین و، وردەکاری تەواو ناخەینە روو لە بارەیەوە:

١. ئەدوێر Adware: کورتکراوەی بەرنامەی پالّپشتی کردنی ئاگانامەییە – Advertising Supported Software ، و جۆرێکی مالّویرە کە ئاگانامەدادەنێت بەشێوەیەکی خۆکاری، واتە بەرنامەی ئاگانامەیی بێزارکەرە و، کەمترین ترسناکی و زۆرترین قازانجی هەیە، ئەدوێر ریکلام و ئاگاداری پیشان دەدات لەسەر کۆمپیوتەری بەرامبەر.

٢. بووت Bot: ئەو بەرنامانەیە کە دروستکراوە بۆ جیبەجیکردنی کارێکی دیاری کراو، بە شێوەیەکی خۆکار. لەکاتێکدا هەندێك لە بوتەکان دروستکراون بۆ هەندێك کار و بەشێوەیەکی رێژەیی بێزیانن. وەکو یاری ڤیدیۆیی Video Gaming و، بانگەوازی ئاشکرایی ئینتەرنێتی، پێشبڕکێی راستەوخۆ و ئۆن لاین.

٣. رووتکیت Rootkit: جۆرێکی مالۆێرە و، درووستکراوە بۆ مەبەستی دەستپێگەیشتن و دەست بەسەراگرتن لە دوورەوە، بە بێ ئەوەی پێی بزانرێت لەلایەن بەکارهێنەرەوە یان بەهۆی بەرنامەکانی پاراستنەوە.

نیشانەکانی مالۆێر

Malware Symptoms

لە کاتێکدا جۆرەکانی مالۆێر ، جیاوازییەکی زۆر هەیە لە نێوانیان دا، لە رووی چۆنێتی بلاوبوونەوە و جێگیر کردنیان لە سەر ئامێری کۆمپیوتەر، بەلام هەموویان دەبنە هۆکاری رووداو و بەرهەم هێنانی نیشانەیی لێکچوو، کە کۆمپیوتەر تووش دەکەن Infected و، ئەم نیشانانەی لای خوارەوە لەسەر ئامێرە تووشبووەکە دەردەکەوێت:

١. بەکارهێنانی یەکەی چارەسەر کردنی ناوەندی CPU=Central Processing Unit زیاد دەکات و مەشغوولی دەکات.
٢. خێرایی وێبگەر Browser Speed و کۆمپیوتەر Computer کەمدەکاتەوە.
٣. گرفت لە پێکەوە بەستن و گریدان بە رایەڵەوە درووستەکات.
٤. ویرانکاری رووەدات.
٥. فایلەکان دەسرێتەوە یان گۆرانکاری بچووکی تیا دەکات.
٦. دەرکەوتنی فایل و بەرنامە و ئایکۆنی عەجیب و غەریب.
٧. بەرنامەی چالاك و کارپێکردوو دەوەستێنێت و هەندیك جار دای دەخات و دەیکاتەوە و .... .
٨. بەهۆیەوە رەفتاری عەجیب و غەریب رووەدات لە کۆمپیوتەردا.
٩. ئیمەیل و نامە و پەیام دەنێردرێت بێ ئەوەی نیرەرەکەی دیار بێت و بزانرێت، یاخود هاورێکەت نامەی

عەجیب و غەریب وەرەگرێت لە تۆوە و لە کاتێکدا تۆش نەت ناردووە.

خۆپاراستن لە مالوێر و لابردنی

Malware Prevention & Removal

چەند رێگەیەکی جیاوازیی پاراستنی کرداریی گشتی هەیە، کە رێکخراوەکان و بەکارهێنەرەکان دەتوانن بەکاری بهێنن و بیگرنە بەر بۆ خۆپاراستن و دوورکەوتنەوە لە تووشبوون بە مالۆێر، بەڵام هەندێك لە مالۆێرەکان پێویستیان بە رێگەی پاراستن و چارەسەرکردنی تایبەتی هەیە، ئەمانەی لای خوارەوە پاراستنی بەکارهێنەر زیاد دەکەن بۆ دوورکەوتنەوە لە تووشبوون بە مالۆێرەکان:

١. دابەزاندن و بەکارهێنانی دژە مالۆێر Anti Malware، هەروەها بەرنامەی دیواری ئاگرین Firewall Software، وەلێ پێویستە ئەو بەرنامەیە هەلبژێرین کە خزمەتگوزاری پێشکەش دەکات بۆ دۆزینەوەی جۆری جیاوازی مالۆێر و هەروەها لابردن و چارەسەر کردنیان، لانی کەم، بەرنامەی دژە مالۆێر پێویستە پارێزگاری بکات دژی ((ڤایرۆس Virus، بەرنامەی جاسووسی Spy Ware، ئەد وێر Adware، ئەسپی تەروادە Trojan Hourse، و کرمەکان Worms. خۆ ئەگەر بەرنامەکە پێکهاتبێت لە دژە مالۆێر و دیواری ئاگرین پێکەوە، ئەوە زۆر باشترە لە رووی پاراستنەوە.
٢. نوێکردنەوە Update ی بەرنامە و سیستەمی کارپێکردن بۆ پینەکردنی خاڵە لاوازەکان، و نەهیشتنی لاوازی و بەهێز کردن، ئەمەش دەمان پارێزێت لە هێرشەکان.
٣. پێویستە بە ئاگاییەوە فایل و بەرنامە و هاوپێچەکان وەربگرین Download بۆ ناو کۆمپیوتەرەکەمان، لەسەرچاوەی باوەرپێکراوەوە دای ببەزێنین.

ناوەندی کردار

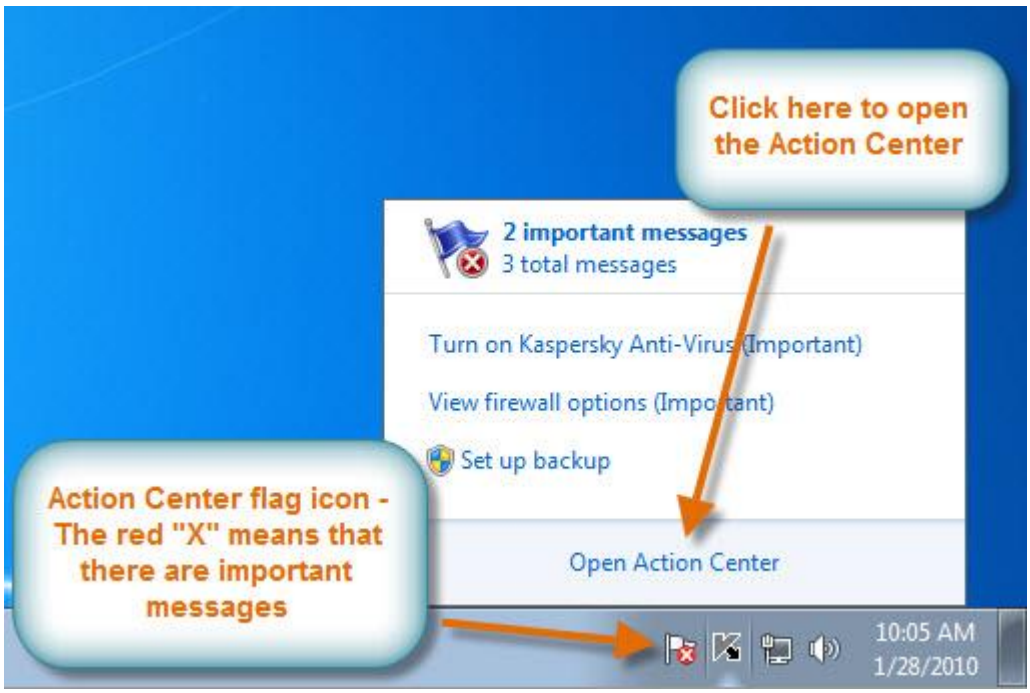
Action Center

ناوەندی کردار Action Center: بەناوەندکردنی شوێنێکە بۆ پیشاندانی نامە و پەیامی مانەوە و پاراستن Security and Maintenance Message، ئەمەش کار ئاسانی دروستەکات بۆ دۆزینەوە و چارەسەر کردنی کێشە کان لە کۆمپیوتەر دا.

بەکارهێنانی ناوەندی کار

Use Action Center

بۆ کردنەوەی ناوەندی کار، کلیك لەسەر ئالا بچوکەکەی سەر شریتی گرنگییەکان Task Bar دەکەین.پاشان نامە و پەیامەکە ئەخوینینەوە، پاشان کلیك لەسەر کردنەوەی ناوەندی کار Open Action center دەکەین:



کردنەوەی ناوەندی کار لە پەنیڵی دەست بەسەرا گرتنەوە

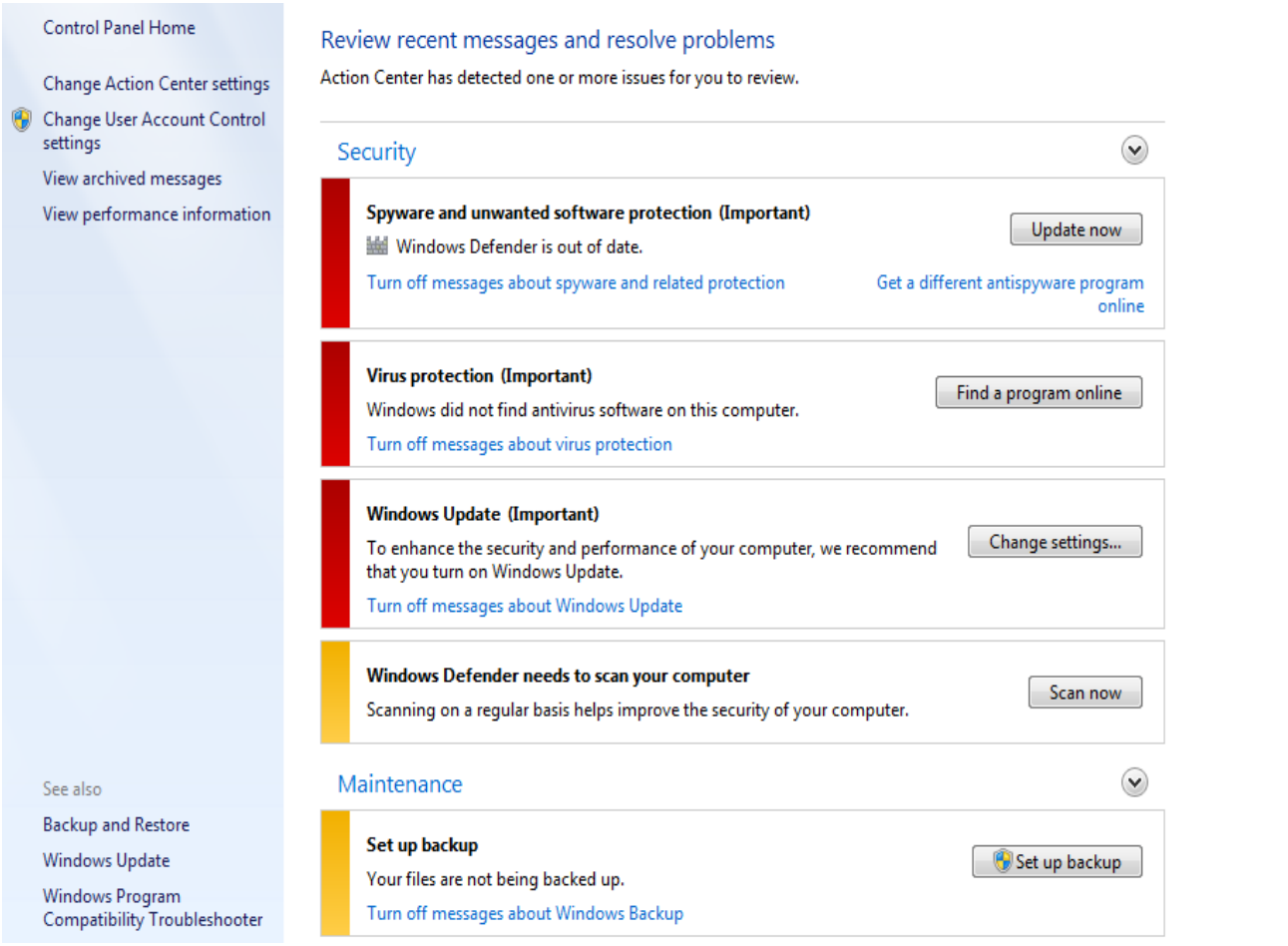
Open Action Center from Control Panel

١. کلیك لەسەر دووگمەی دەستپێکردن Startدەکەین.
٢. کلیك لەسەر پەنێڵی دەستبەسەرا گرتن Control Panelدەکەین.
٣. سیستەم System دەکەینەوە.
٤. پاشان کلیك ناوەندی کار Action Center دەکەین.

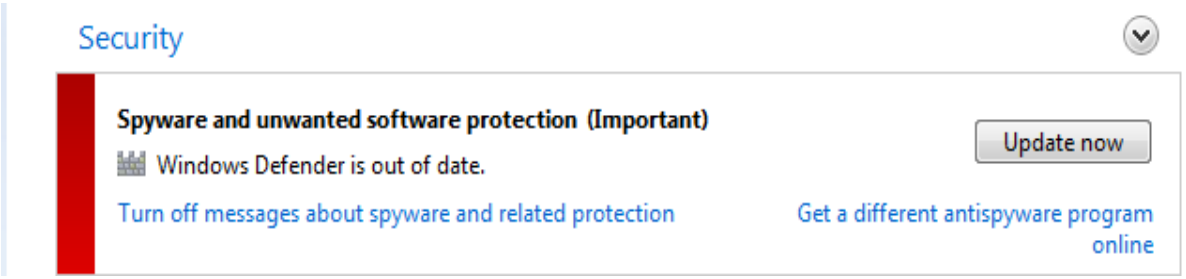
دیاری کردنی کێشەکان

Fixing Problems

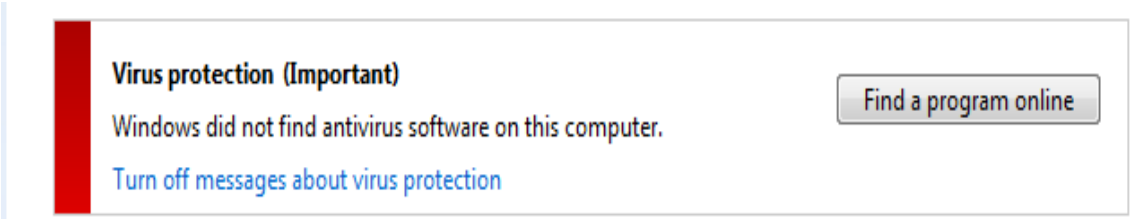
نامە و پەیامەکان لە ناوەندی کار دا پیشان دەدرێت، گرنگترین نامە و پەیامەکان شریتە سورەکەیە Red Bar، بەلام شریتە زەردەکە Yellow Bar کەمتر گرنگە، بۆ دیاری کردنی کێشەکان ، ((شیکار)) Solution ئەنجام دەدەین:



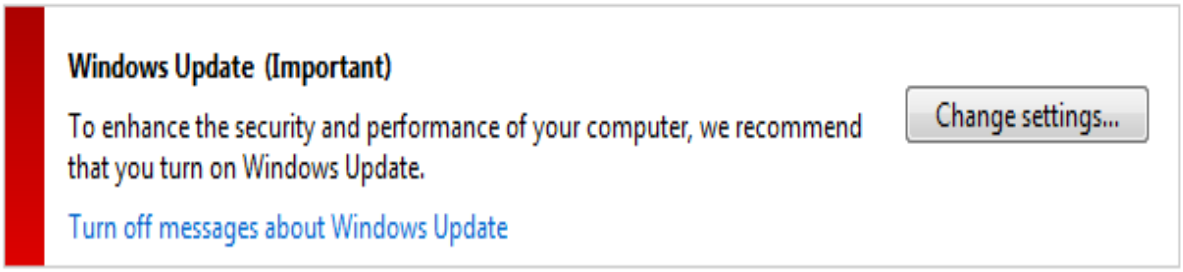
- بۆ چارەسەر کردنی بەرنامەی جاسووسی و ئەو بەرنامانەی کە نامانەوێت و خۆپاراستن لێیان، نوێکردنەوەی هەنووکەیی Update Now ئەنجام دەدەین:



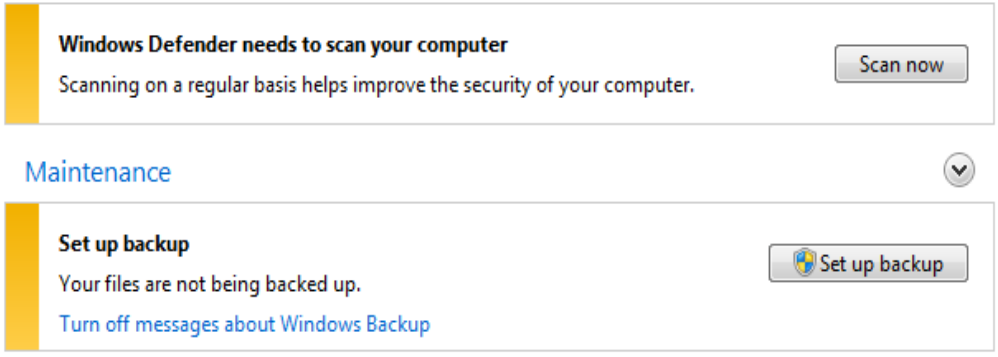
- بۆ پارێزەری ڤایرۆس Virus Protection، بەرنامەی دژە ڤایرۆس ئەدۆزینەوە لە رێی ئینتەرنێتەوە و کلیك لەسەر Find Program Onlineدەکەین:



- بۆ فراوان کردنی پاراستن و باشتر کردنی چوستی سیستەمی کارپێکردن Operating System نوێدەکەینەوە و هەلبژاردن و رێکخستنەکان دەگۆرین.



- بەرنامەی ویندۆز دیفیندەر Windows Defender پێویستە بۆ پشکنینی کۆمپیوتەرەکەمان و، بە کلیك کردن لە سەر دووگمەی پشکنینی هەنووکەیی Scan Now سودی لێوەرەگرین.
- بەشی نووسخەی یەدەگ Back up پێمان دەلێت کە نووسخەی یەدەگی فایلەکەمان هەلنەگرتووە.



دەست بە سەرا گرتنی ئەژماری بەکارهێنەر

User Account Control

دەست بەسەراگرتنی ئەژماری بەکار هێنەر User Account Control ئاگاداریت پێدەدات کاتێك بەرنامە Program یان بەکارهێنەر هەوڵدەدات بۆ گۆرینی رێکخستن و تایبەتمەندی کۆمپیوتەرەکەت، ئەمەش دانانی داخستنێکی کاتی یە لە سەر کۆمپیوتەرەکەت Temporary Lock هەتاوەکو پشت راستی نەکەیتەوە Confirm گۆرانکاری روونادات، ئەمەش یارمەتی پاراستن دەدات دژی مالۆێرەکان .

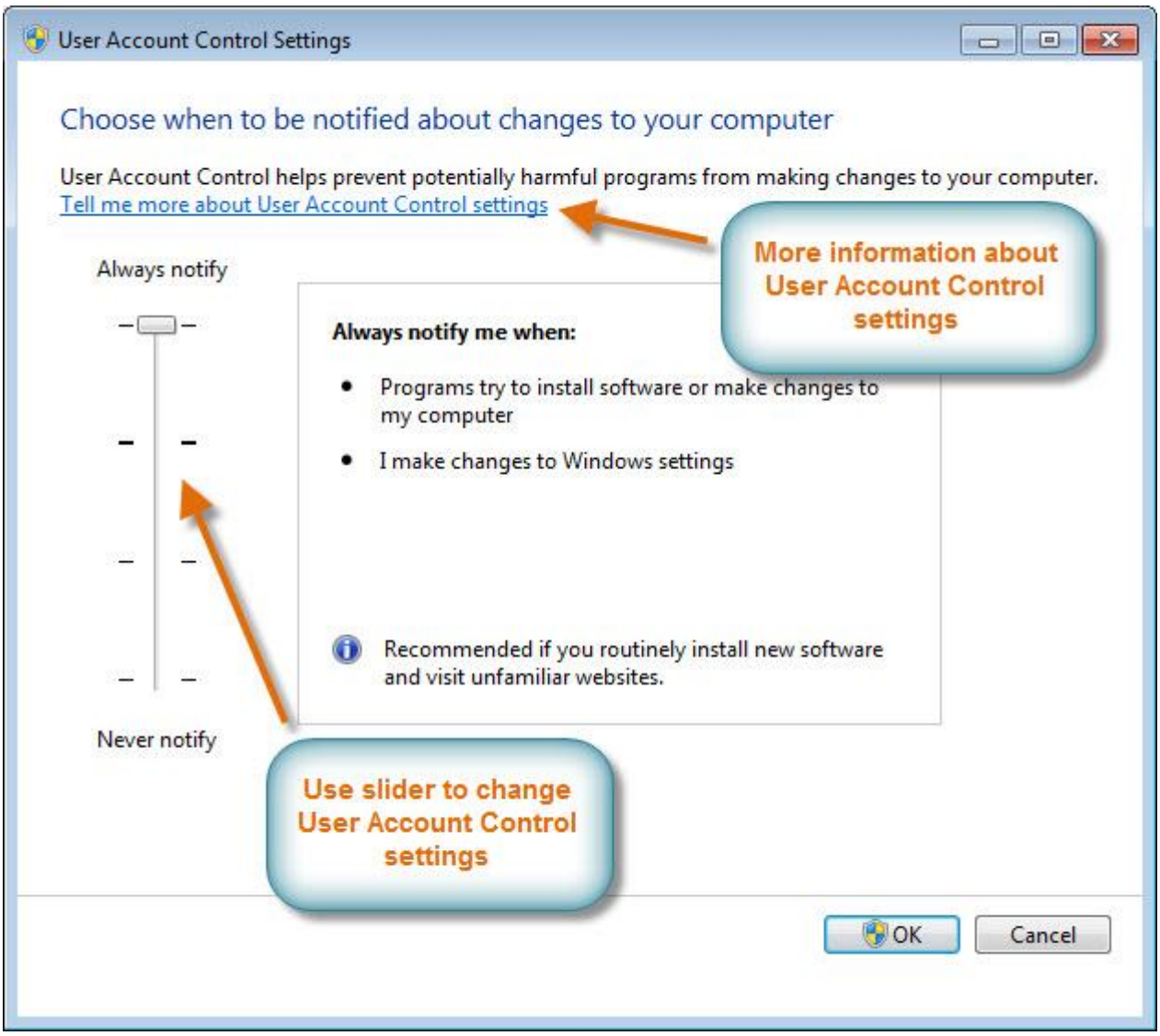
رێکخستنی دەست بە سەراگرتنی ئەژماری بەکارهێنەر

User Account Control Setting

١. سەنتەری کار Action Center بکەرەوە.

٢. لە بەشی لای دەستە چەپ و لای سەرەوە کلیك لەسەر Change User Account Control Setting بکە.

۳. سلایدەرەکە بەکار بهێنە بۆ گۆڕینی ئاستی پاراستنەکە



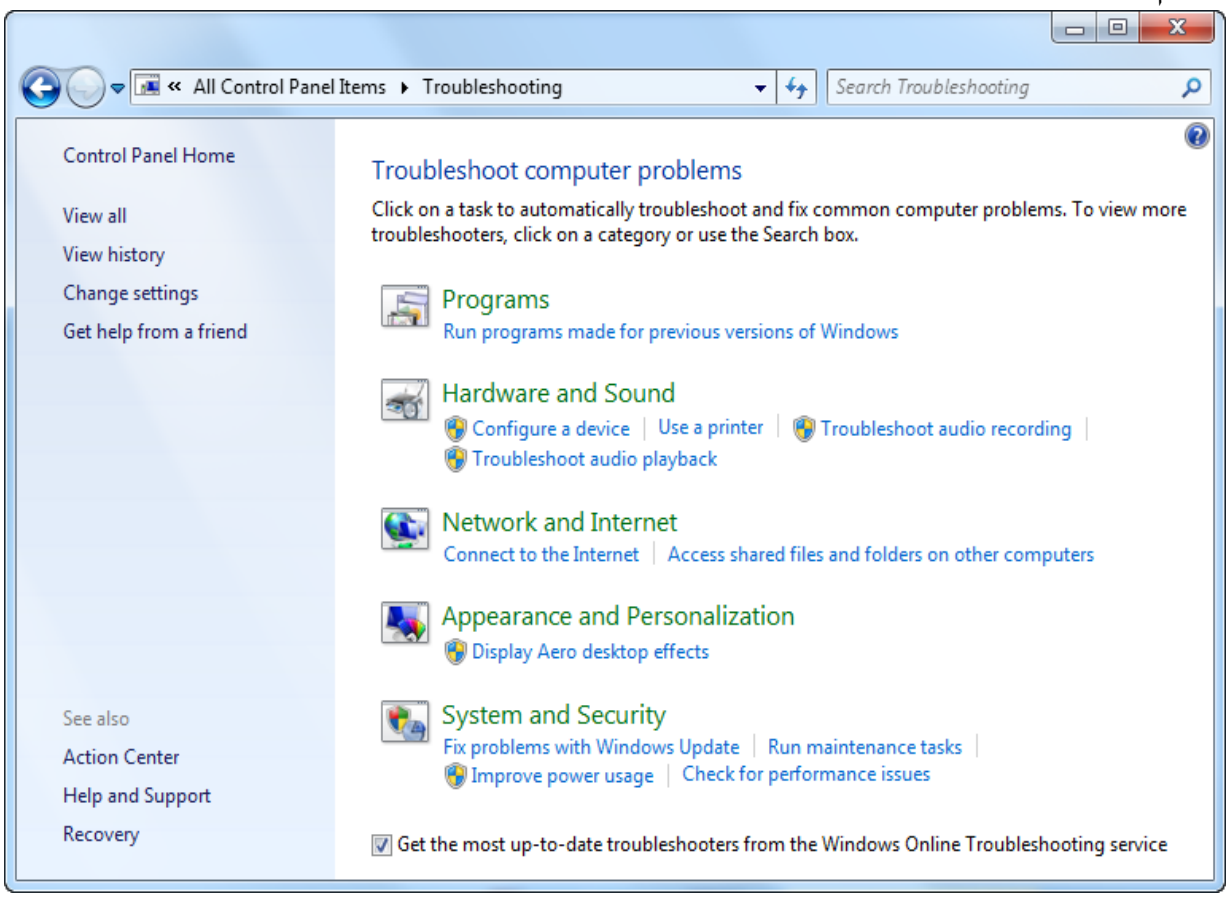
دۆزینەوەی هەڵە و چارەسەر کردنی

Troubleshooting

۱. ناوەندی کار Action Center بکەرەوە.

۲. لەبەشی خوارەوە ی دا، کلیك لەسەر Troubleshooting بکە.

٣. ئەم رووکارەی لای خوارەوە دەکرێتەوە:



بەشی پاراستن و سیستەم System and Security هەلبژاردنێکە بەکاردێت بۆ چارەسەر کردنی کێشە و گرفتەکان لەگەڵ نوێترین تازەکردنەوەی ویندۆز Windows Update، هەروەها بۆ جێبەجێکردنی کردارەکانی چاککردنەوە .

پاراستن و چاککردنەوە

Security and Maintenance

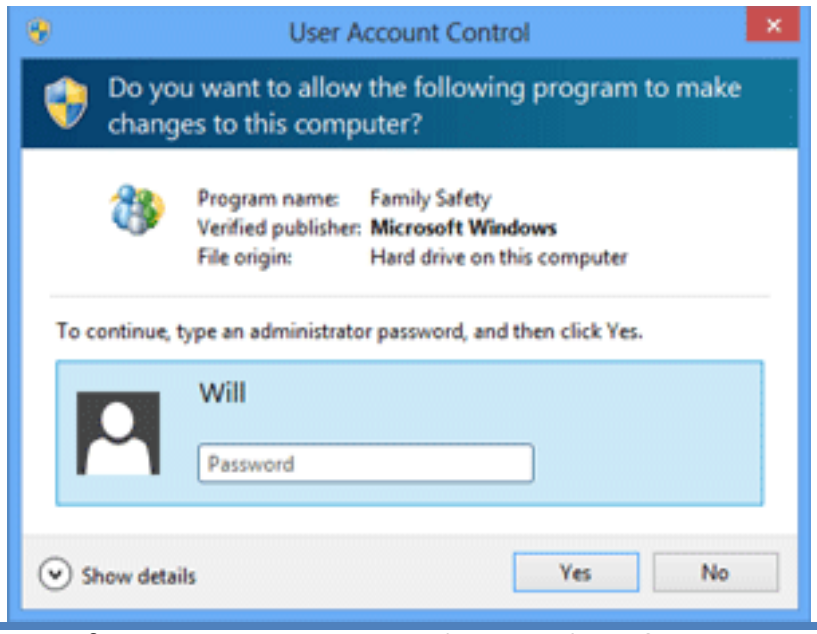
لەم بابەتەدا باس لە وە دەکەین کە چۆن ویندۆز هەشت Windows 8 کۆمپیوتەر دەپارێزێت، و تایبەتمەندییەکانی پاراستن روون دەکەینەوە.

تایبەتمەندییەکانی پاراستن لە ویندۆز هەشت دا

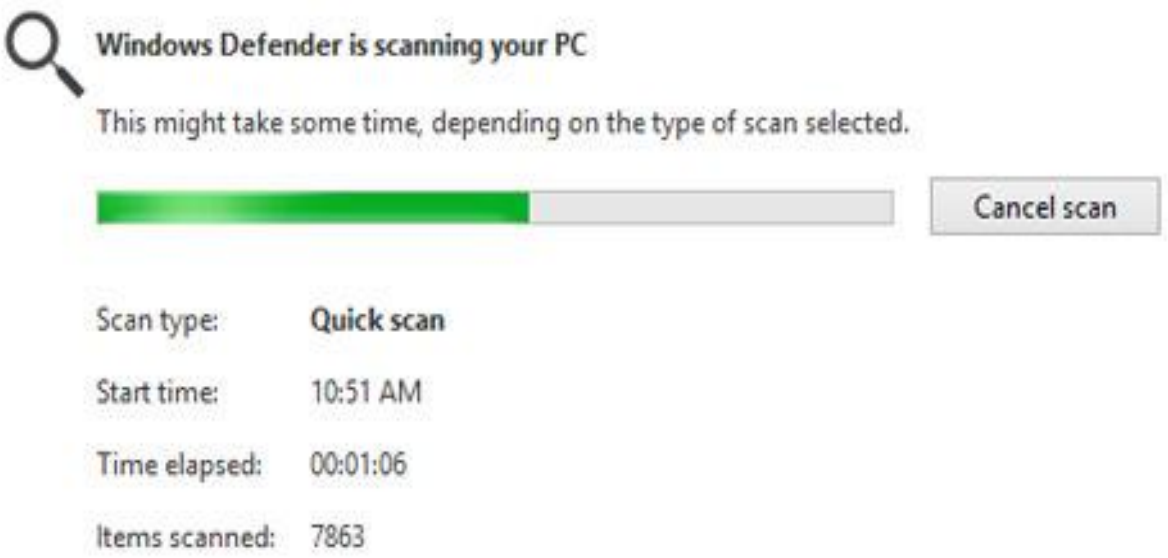
Security Featuers in Windows 8

ویندۆز هەشت ئامرازی جیاواز و جۆراو و جۆر هەیە بۆ پاراستن، و دژی ڤایرۆسەکان Viruses، مالوێر Malare، و بەرنامە پیس و خراپەکانی تر Other Malicious Application، کە مەترسین بۆ سەر کۆمپیوتەر، هەندێك لەو خزمەتگوزارییانە لە پشتەوە جیبەجێدەبن Run in Background. بە کورتی باس لەو تایبەتمەندییانە دەکەین کە پاراستنن لە ویندۆز هەشت دا.

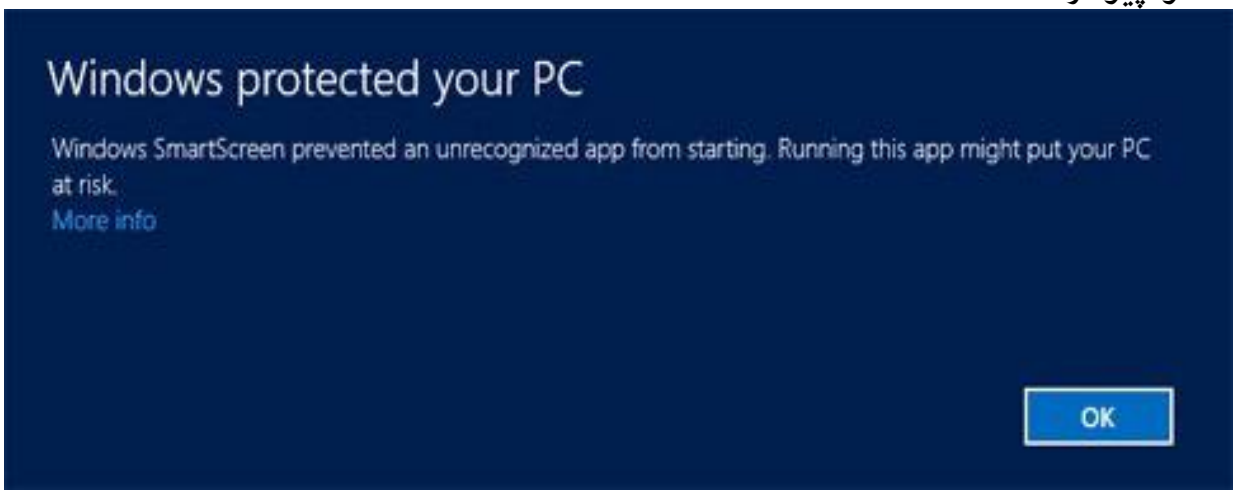
١. دەستبەسەراگرتنی ئەژماری بەکارهێنەر User Account Control: دەست بەسەراگرتنی ئەژماری دەست بەسەراگرتن ئاگاداری و بیرخستنەوە دەدات لەکاتێکدا بەرنامە یان بەکارهێنەر هەولبدات بۆ گۆڕینی ڕێکخستن و تایبەتمەندی کۆمپیوتەر، شاشەکەت بە شێوەیەکی کاتی دەوەستێت Temporarly Locked، هەتاوەکو بەڕیوەبەر ئەو بەکارهێنانە پشت ڕاست دەکاتەوە و ڕەزامەندی دەدات لەسەر گۆڕانەکە، ئەم یارمەتی یە بۆ پاراستنی کۆمپیوتەرە دژی مالوێر Malicious Software، و گۆڕانە ڕێکەوت و لەپەرەکان Accedental Changes:



٢. بەرنامەی ویندۆز دیفیندەر Windows Defender: بەرنامەی ویندۆز دیفیندەر دژە ڤایرۆسەکان و پاراستنی مالوێر Anti-Viruses and Malware Protection، دابین دەکات بۆ پاراستنی کۆمپیوتەرەکەمان، هەروەها بۆ پشکنینی کۆمپیوتەرەکەمان دژی بەرنامە زیان بەخشەکان، ویندۆز دیفیندەر پاراستنی کاتی راستەوخۆ Real – Time Protection دابین دەکات.



٣. شاشەی زیرەکی ویندۆز Windows Smart Screen: هەرکاتێك کۆمپیوتەر هەڕەشەی پاراستنی ئاشکرا کرد، لە فایلێکەوە یان لە بەرنامەیەکەوە، ئەوا شاشەی پاراستنی زیرەك سەرنج و تیبینیمان دەداتێ بە ئاگانامەیەکی پرا و پری شاشە، هەر کاتێك ئەم ئاگانایەت بینی پێویستە فایل یان بەرنامە دابخەیتەوە و نەیکەیتەوە، بەمەش کۆمپیوتەرەکەت دەپارێزیت و گۆران رووناداتە لە کۆمپیوتەرەکەدا:



٤. دیواری ئاگرینی ویندۆز Windows Firewall: بەشێوەیەکی هەمیشەیی ویندۆز هەشت پێکەوەبەستن و گرێدانی ئینتەرنێت Internet Connectionدەپارێزێت، بە بەکارهێنانی دیواری ئاگرینی ویندۆز، دیواری ئاگرین رێگە دەگرێت لە دەستپێگەیشتنی رێگەپێنەدراو، لە کاتی پێکەوەبەستنی دەرەکی، هەروەها پاراستنی رایەڵە لە هەرەشەکان کە دەبنە زیان بۆ کۆمپیوتەر.

ناوەندی کردار

Action Center

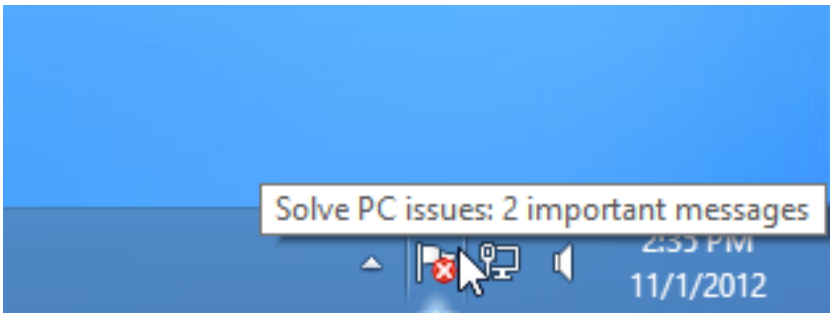
ناوەندی کردار Action Center: بەناوەندکردنی شوێنێکە بۆ پیشاندانی نامە و پەیامی مانەوە و پاراستن Security and Maintenance Message، ئەمەش کار ئاسانی دروستەکات بۆ دۆزینەوە و چارەسەر کردنی کێشە کان لە کۆمپیوتەر دا.

بەکارهێنانی ناوەندی کار

Use Action Center

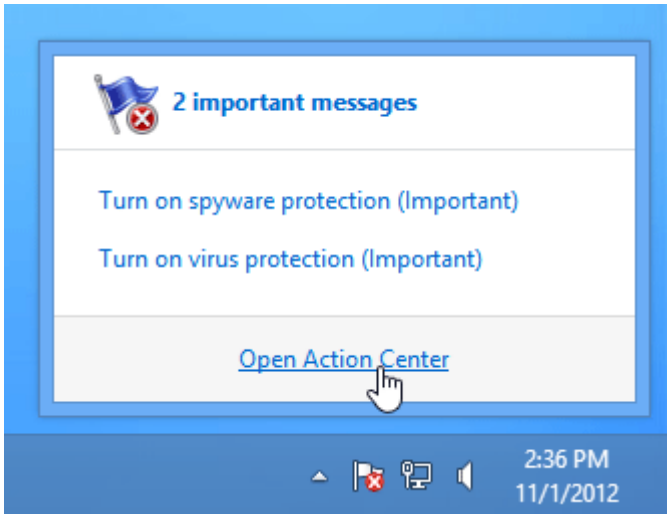
بۆ کردنەوەی ناوەندی کار:

١. کلیك لەسەر ئالا بچوکەکەی سەر شریتی گرنگییەکان Task Bar دەکەین.



٢. پاشان نامە و پەیامەکە ئەخوینینەوە.

٣. پاشان کلیك لەسەر کردنەوەی ناوەندی کار Open Action centerدەکەین:



کردنەوەی ناوەندی کار لە پەنیڵی دەست بەسەرا گرتنەوە

Open Action Center from Control Panel

٥. کلیك لەسەر دووگمەی دەستپێکردن Startدەکەین.

٦. کلیك لەسەر پەنێڵی دەستبەسەرا گرتن Control Panelدەکەین.

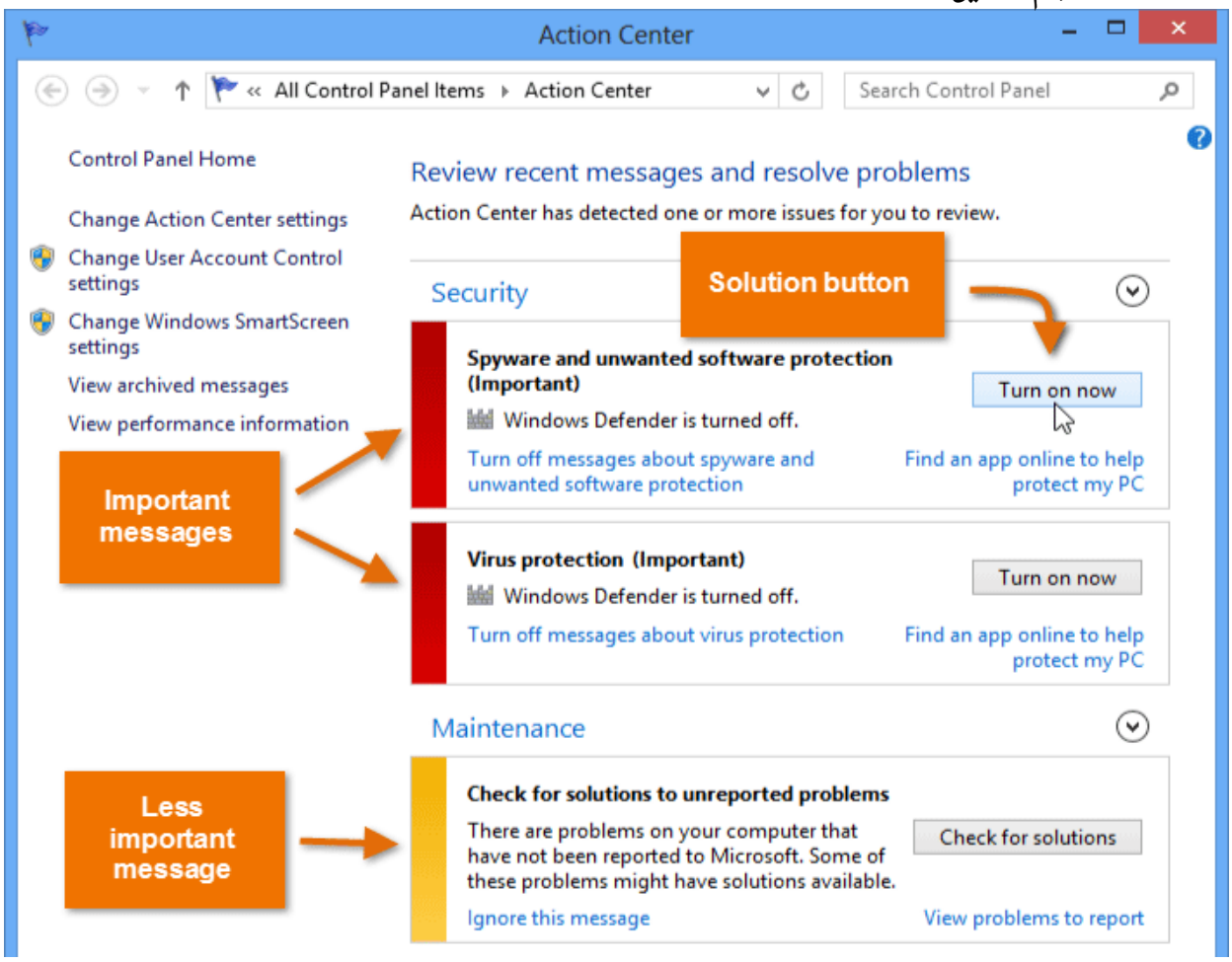
٧. سیستەم System دەکەینەوە.

٨. پاشان کلیك ناوەندی کار Action Center دەکەین.

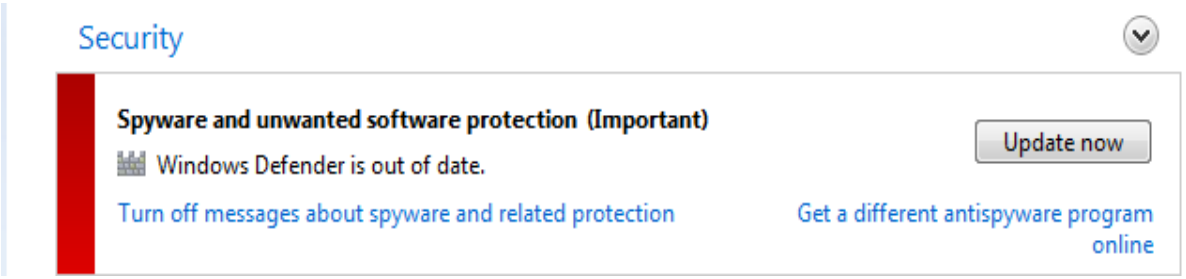
دیاری کردنی کێشەکان

Fixing Problems

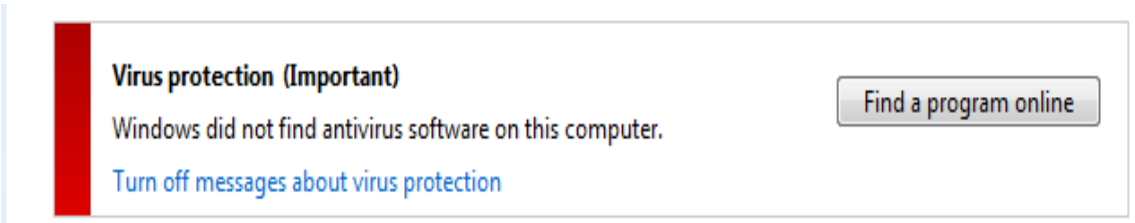
نامە و پەیامەکان لە ناوەندی کار دا پیشان دەدرێت، گرنگترین نامە و پەیامەکان شریتە سورەکەیە Red Bar، بەلام شریتە زەردەکە Yellow Bar کەمتر گرنگە، بۆ دیاری کردنی کێشەکان ، ((شیکار)) Solution ئەنجام دەدەین:



- بۆ چارەسەر کردنی بەرنامەی جاسووسی و ئەو بەرنامانەی کە نامانەوێت و خۆپاراستن لێیان، نوێکردنەوەی هەنووکەیی Update Now ئەنجام دەدەین:



- بۆ پارێزەری ڤایرۆس Virus Protection، بەرنامەی دژە ڤایرۆس ئەدۆزینەوە لە رێی ئینتەرنێتەوە و کلیك لەسەر Find Program Onlineدەکەین:



بەشی سێیەم

کریپتۆگرافی

Cryptography

کریپتۆگرافی زانی

Cryptology

کریپتۆگرافی زانی یان زانستی کریپتۆگرافی Cryptology، ڕشتەی کریپتۆگرافی Cryptography یە، لێکۆڵینەوە و بەوردی تێڕوانینی سیستەمی کریپتۆیە Cryptosystem، گونجاوە دابەش بکرێت بۆ دوو پسپۆڕیی، کریپتۆگرافی گرنگی دەدات بە نەخشە سازیی سیستەمی کریپتۆگرافی Cryptosystem، لەکاتێکدا شیکارکەری کریپتۆگرافی Ctyptoanlysis رشتە و لێکۆڵینەوەی تێکشکاندنی سیستەمی کریپتۆگرافی Cryptosystem یە. ئەم دوو بوارەش پەیوەندی دارن بەیەکەوە و، شیکار کەری سیستەمی کریپتۆگرافی Cryptosystem analysis، رۆلێکی زۆر گرنگی هەیە لە پاراستنی زانیاری دا.

کریپتۆگرافی

Cryptography

کریپتۆ گرافی Cryptography: پرۆسەی جیبەجێکردن و گۆڕینی زانیارییە بۆ شێوەیەك، کە نەخوێندرێتەوە Unreadable و، کەس لێی تێنەگات کاتێك دەیبینێت. ئەمەش ئەنجام دەدرێت بۆ مەبەستی پاراستنی زانیاری Information Security، و دوورخستنەوەی زانیاری ورد و گرنگ لە دەستی هەر کەسێك کە مەبەستی بێت و بیەوێت بیخوێنێتەوە.

پێناسەکان و زاراوەزانی

Deffinitions and Terminology

- بە هێما کردن Ecryptionالتشفیر : کرداری بەهێماکردنی نامە و پەیامەکانە بۆ ئەوەی زانیارییەکەی بشاردرێتەوە و هیچ کەسێك لێی تێنەگان جگە لەو کەسەی نامە و پەیامەکەی بۆ ئەچێت و تایبەتە بەو کەسە.
- گۆڕینەوەی بەهێماکراو Decryption: بریتییە لە کرداری وەرگرتنی نووسینی بەکۆد کراو

Encoded Text، یان نووسینی بەهێماکراو Encrypted Text یان زانیاری شیکارنەکراوی تر Other Data، هەروەها گۆڕینەوەی بۆ نووسینی ئاسایی Plain Text کە تۆ یان کۆمپیوتەر بۆی بخوێندرێتەوە و لێی تێبگات، ئەم زاراوەیە بەکاردەهێنرێت بۆ وەسفکردنی ڕێگەی گۆڕینەوەی نووسینی بەهێماکراو بۆ نووسینی ئاسایی.بە بەکارهێنانی کۆدێکی دیاری کراو، یان کلیلەکان Keys. زانیاری لەوانەیە بکرێتە هێما بۆ مەبەستی پاراستنی زانیاری لە دزین، هەندێك کۆمپانیا بە هێماکردن بەکاردەهێنێت بۆ مەبەستی پاراستنی کۆمپانیاکە بەشێوەیەکی گشتی.

- ڕێککەوتننامە Protocol: ئەلگۆریسمە، دیاری دەکرێت بەهۆی زنجیرەیەك هەنگاوەوە، هەروەها دیاری کردنی کردارەکانە بە بەجێگەیاندنی ئامانجێك.
- نووسینی ئاسایی Plaintext: نامە و پەیامێکە کە دەگوێزرێتەوە یان پاشەکەوت دەکرێت.
- نووسینی بە هێماکراو Cipher Text: ئەو نامە و پەیامەیە کە کراوەتە هێما و ئەگەر دەست کەسێك بکەوێت بیزار دەبێت لێی و لێی تێناگات.
- ئەلفبێ Alphabet: کۆمەلێك هێمایە، کە کارەکتەرەکانیان پێ ئەلێن.
- کارەکتەر Character: دانەکانی ئەلف بێ یە.
- بت ((تڕپە، لێدان)) Bit: سفر ((٠)) یان یەکە ((١)).
- زنجیرە String: زنجیرەیەك کارەکتەرە پێکەوە.
- سایفەر Cipher: نووسینی ئاسایی Plainn Text بۆ نووسینی هێمایی Cipher Text.
- بە هێماکردن Encipher: کرداری گۆڕینی نووسینی ئاساییە Plain Text بۆ نووسینی هێمایی Cipher Text.
- گۆڕینەوەی بە هێماکراو Decipher: کرداری گۆڕینەوەی نووسینی بە هێماکراوە Cipher Text بۆ نووسینی ئاسایی Plain Text.
- جۆگەلەی هێما Stream Cipher: سایفەر کاردەکات لەسەر یەك هێمای نووسینی ئاسایی لە هەمان کات دا.
- سایفەری دابڕشتگەیی((قاڵبی/ بلۆك)) Block Cipher: سایفەر کاردەکات لەسەر کۆمەلێك لە پیت.
- سایفەری خستنە جێ Sustitution Cipher: سایفەری جۆگەلەییە Stream Cipher کە کاردەکات لەسەر نووسینی ئاسایی بەهۆی ئاڵوگۆڕی کارەکتەرەکان لەگەڵ دانەی نوێی ئەلف بێ.
- سایفەری جێگۆڕکێ Transposition Cipher: سایفەری بلۆك Block Cipher کە کاردەکات لەسەر نووسینی ئاسایی بە گۆڕینی شوێنی کارەکتەرەکان Position of Character، لە نووسینی ئاسایی Plain Text.

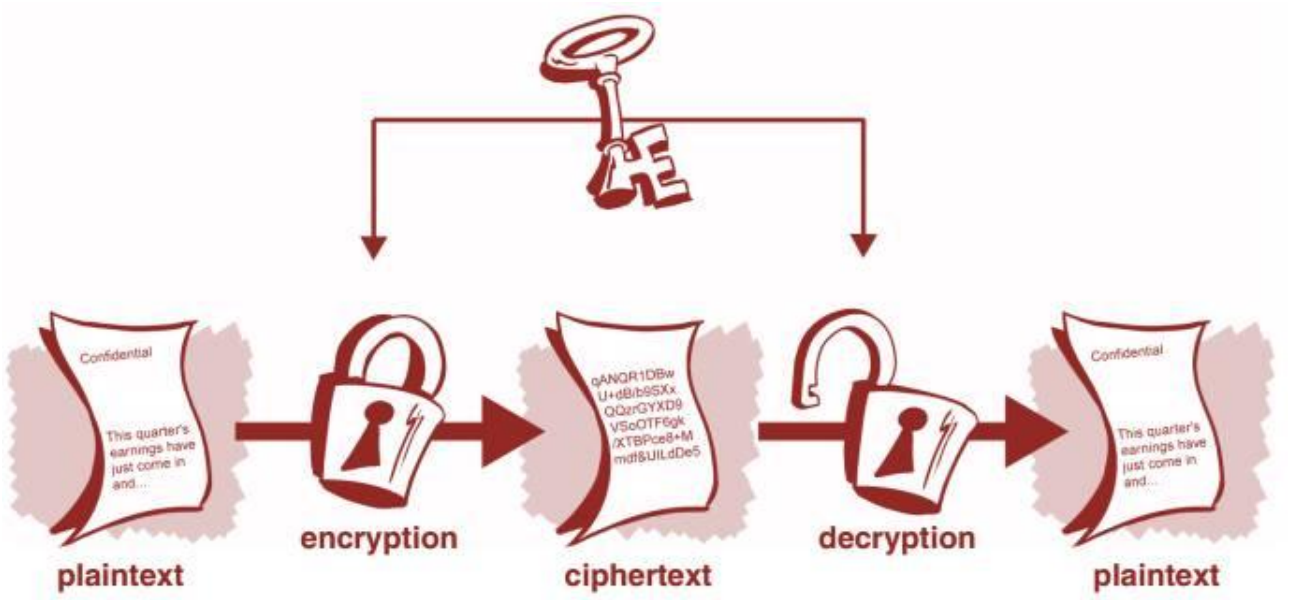
-

کریپتۆسیستەم

Cryptosystem

سیستەمی کریپتۆگرافی یان کریپتۆ سیستەم، دووانە ئەلگۆریسمە Pair of Algorithms کە بە وەرگرتن و بەکارهێنانی کلیلێك Key نووسینی ئاسایی Plain Textدەگۆڕێت بۆ نووسینی هێمایی Cipher Text و ، پێچەوانە کردنەوەشی ئەنجام دەدات واتە سایفەر ((نووسینی هێمایی)) Cipher Text دەگۆڕێتەوە بۆ نووسینی ئاسایی Plain Text.

هەرچی نووسینی ئاساییە Plaint Text ئەو نووسینەیە کە دەمانەوێت بیپارێزین Protect و، سایفەریش Cipher Text ئەو نووسینەیە کە پارێزراوە Protected بەهۆی یەکێك لە ئەلگۆریسمەکانی گۆڕینی نووسینی ئاسایی بۆ سایفەر، هەروەها دووانر پێچەوانە کردنەوە و گۆڕینەوەی سایفەر بۆ نووسینی ئاسایی.



ئەلگۆریسمەکانی کریپتۆگرافی

Cryptography Algorithms

ڕێگەکانی بەهێماکردن Encryption و گۆڕینەوەی بەهێماکردنەکە بۆ نووسینی ئاسایی Decryption بریتی یە لە سافەر Cipher، بەشێوەیەکی گشتی ئەم ئەلگۆریسمانە دابەش دەکرێن بۆ ئەلگۆریسمە هاوتا و

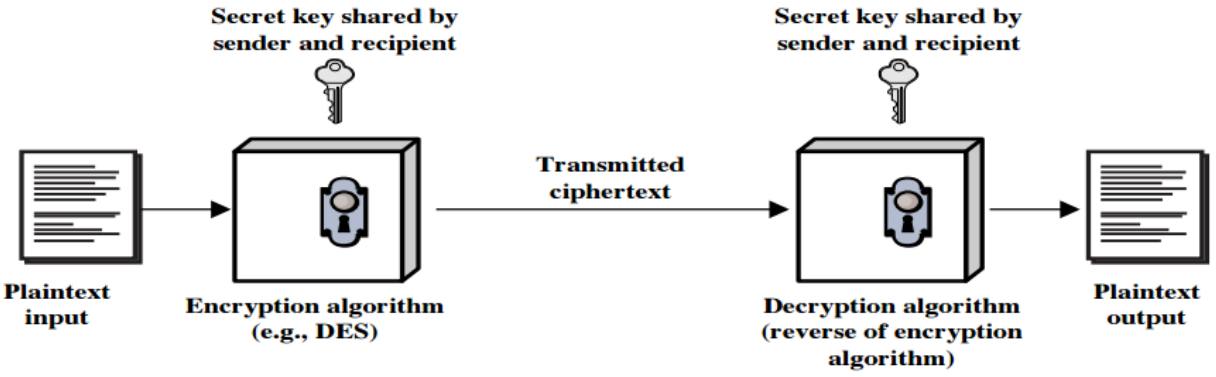
بەرامبەرەکان Symmetric Algorithm بە بەکارهێنانی کلیلی شاراوە Secret Key، هەروەها ئەلگۆریسمە ناهاوتا و نابەرامبەرەکان Asymmetric Key بە بەکارهێنانی کلیلی گشتی Public Key.

بەهێماکردنی هاوتا

Symmetric Encryption

بەهێما کردنی هاوتا Symmetric Encryption بریتییە لە کرداری گۆڕینی نووسینی ئاسایی Plain Text کە زانیارییەکە دەخوێنرێتەوە Redable Data، بۆ نووسینێك کە هێمایە Cipher Text و، زانیارییەکە ناخوێندرێتەوە Unredable Data، بە بەکارهێنانی هەمان کلیل Using Same Key، بۆ هەردوو کردارەکە.

ئەلگۆریسمەکانی بەهێماکردنی هاوتا Symmetric Encryption Algorithm، هەمان کلیل Same Key بەکاردەهێنێت بۆ بەهێماکردن Encryption و، پێچەوانەکردنەوەی ئەو بەهێماکردنە Decryption و، گێرانەوەی بۆ هەمان نووسینی ئاسایی. ئەم کلیلەش پێویستە ئالوگۆر بکرێت لە نێوان نێرەر Sender و وەرگر Receiver.



ئەلگۆریسمەکانی بەهێماکردنی هاوتا

Symmetric Encryption Algorithms

١. بەهێماکردنی پێوانەیی زانیاری (Data Encryption Standard (DES: ئەلگۆریسمی بەهێماکردنە Encryption Algorithm کە زانیاری ئاسایی و خوێنراوە دەکاتە هێما، بە بەکارهێنانی ٥٦-بت، بەشێوەیەکی هەرەمەکی کلیلی هاوتا Symmetric Key دروست دەکات، ئەلگۆریسمی دی ئی ئیس DES دروستکراوە لە لایەن کۆمپانیای ئی بی ئێم IBM Company و حکومەتی ویلایەتە یەکگرتووەکان پێکەوە، دی ئی ئیس لە ئەلگۆریسمی جۆری کۆمەڵە (بلۆك) Blockیە .

٢. دی ئی ئیس ئێکس DESX، کورتکراوەی Data Encryption Standard XORed ـە و، ئەلگۆریسمێکی جۆراو جۆر و بەهێزتری دی ئی ئیسە DES، نووسینی ئاسایی داغڵکراو Input Plain Text ئیکس ئۆری پێدەکرێت XOR لەگەڵ ٦٤ بت لە کلیلی زیادکراو Additional Key پێش ئەوەی بکرێتە هێما بەهۆی دی ئی ئیس-ـەوە، بەهەمان شێوە بەرهەمیش Output ئێکس ئۆری پێدەکرێت لەگەڵ ٦٤ بت لە کلیلێکی تر.

٣. دی ئی ئیسی سیانی 3DES، کە بە Triple DES ناودەبرێت، لە دی ئی ئیسەوە DES بەرهەم هاتووە و پەرە پێدراویی دی ئی ئیسە، بە بەکارهێنانی کلیلی ٦٤ بتی 64-Bit Key، کە پێکهاتووە لە ٥٦ بتی بنچینەیی چالاك و، ٨ بتی تەوازن، لە دی ئی ئیسی سیانی 3DESدا، سێ (٣) جار بەهێماکردنی دی ئی ئیس DES Encryption بەسەر نووسینی ئاسایی Plain Text دا جیبەجێدەبێت. نووسینی ئاسایی Plain Textدەکرێتە هێما لەگەڵ کلیلی ئەی A، پاشان دەگێردرێتەوە بۆ شێوەی ئاسایی بەهۆی کلیلی بی B، جارێکی تر دەکرێتەوە بە هێما بە بەکارهێنانی کلیلی سی C. دی ئی ئیسی سیانی لە جۆری ئەلگۆریسمی بەهیماکردنی داڕشتگەیی ((پارچەیی/قاڵبی)) یە Block Encryption Algorithm.

٤. ئاڕ سی ٢ و، ئار سی ٥ (RC2 and RC5) ڕۆنالد ریڤێست Ronald Rivest ئەم ئەلگۆریسمەی دروستکردووە. ئەم دووانەش لە جۆری ئەلگۆریسمی دارشتگەیی ((قالبی/بلۆك)) یە Block Algorithm، لەگەڵ قاڵبی گۆراو Variable Block و، حەجمەکانی کلیل Key Size، ئەمەش زۆر قورسە بۆ تێکشکاندن ئەگەر هێرشبەرێك حەجمە تەواوە ئەسڵییەکە نەزانێت، کاتێك هەوڵدەدرێت بە هێماکردنەکە لابرێت و نووسینەکە بگەڕێنرێتەوە بۆ سەر شێوەی ئاسایی خۆی.

٥. ئارِ سی چوار (RC4) لە جۆری سایفەری جۆگەلەیی Stream Cipher و حەجمی کلیلەکەی گۆراوە Variable Key Size، لەگەڵ کردارەکانی بایت Byte Operations کارەکە دەکات، ئەم ئەلگۆریسمە لەسەر بنچینەیی بەکارهێنانی هەرەمەکی Random یە، هەروەها بەشێوەیەکی باو بەکاردەهێنرێت بەهێماکردنی جوڵەی مرووز لە سایتەوە یان جووڵەی مرووز بۆ سایتی پارێزراو Traffic to and from secure website، بە بەکارهێنانی رێککەوتننامەی ئیس ئیس ئێل SSL Protocol.

٦. پێوەری بەهێماکردنی پێشکەوتوو Advanced Encryption Standard، بەهێما کردنێکی نوێ و، بەهێزە، کە ئەلگۆریسمی رین-دۆڵ Rijndael، ئەم ئەلگۆریسمە گەشەی پێدراوە لەلایەن Developed جوان دایمن Joan Daemen و ڤنسنت ریجمێن Vincent Rijmen، ئەم ئەلگۆریسمە کۆچکردنێکبوو Displace بە دی ئی ئیس ئیکس DESX و 3DES، واتە ئەو دووانەی لادا و جێگەی گرتنەوە. ئەی ئی ئێس توانای بەکارهێنانی کلیلی ١٢٨-بتی، ١٩٢- بتی و ٢٥٦-بتی هەیە.

٧. ئەلگۆریسی بەهێماکردنی زانیاری نێودەوڵەتی International Data Encryption Algorithm، هاوتا و بەرامبەرێکی Counterpart ئەورووپی یە بۆ ئەلگۆریسمی بەهێماکردنی دی ئی ئێس DES Encryption Algorithm. لە جۆری سایفەری داڕشتگەیی ((قاڵبی)) Block Cipher یە، کە نەخشە سازی بۆ کراوە لە لایەن د.ئێکس.لای Dr.X.Lai و پرۆفیسۆر جەی.ماسێی Professor J.Massey، کاردەکات لەسەر قاڵبی نووسینی ئاسایی شەست و چوار بتی 64-Bit Plain Text Block، هەروەها کلیل ١٢٨بتی.ئەم ئەلگۆریسمە کۆیی هەشت ئەڵقە Eight Rounds لەگەڵ ئیکس ئۆر XOR، کۆکردنەوە Adds و لێکدانی چوار نیمچە بلۆك Four Sub-Block لەگەڵ هەریەکێکیان، هەروەها شەش ١٦-بتی لە کلیلی نیمچە بلۆك Six 16-Bit Sub-Block of Key.

٨. بلۆوفیش Blowfish، سایفەری قاڵبی هاوتایە Symmetric Block Cipher، نەخشە سازیی بۆ کراوە لەلایەن بروس شنیرەوە Bruce Schneier، بلۆوفیش کار بە قاڵبی ٦٤حەجمی بت دەکات 64-Bit Block Size و، کلیلی گۆراو لە نێوان ٣٢ هەتاوەکو ٤٤٨ بت. بروس شنیر Bruce Schneirئەلگۆریسمی تۆوفیش Twofish دروستکرد کە هەمان کاری جیبەجێدەکرد لەگەڵ قاڵبی ١٢٨-بت.

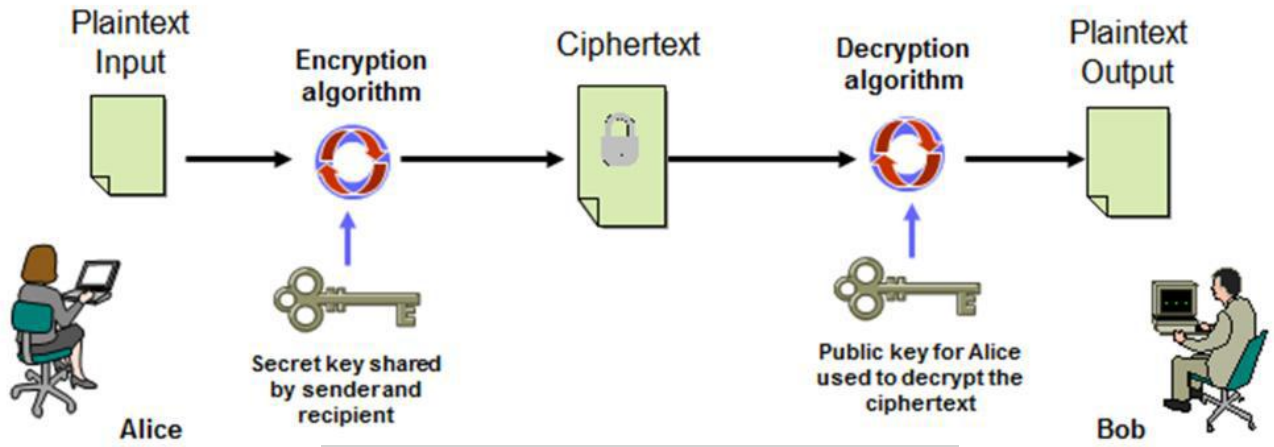
٩. کاست CAST: ئەلگۆریسمێکە دروستکراوە لە لایەن کار لایل ئادەمز Carlisle Adams و، ستافۆرد تاڤاریس Stafford Tavares، ئەم ئەلگۆریسمە لە کۆمەلێك بەرهەمی مایکرۆسۆفت Microsoft و ئای بی ئێم IBMدا، بەکارهاتووە، کاست کلیلی ٦٤بتی تا ١٢٨ بتی بەکار

دەهێنێت. ئەم ئەلگۆریسمە زۆر خێرا و چالاکە.

بەهێماکردنی ناهاوتا

Asymmetric Encryption

بەهێماکردنی ناهاوتا Asymmetric Encryption پاراستن و پرۆسەی بەهێماکردن زیاد دەکات بەهۆی بەکارهێنانی دوو کلیلی جیاواز، بەلام پەیوەندی بیرکارییانە Mathematically هەیە لەنیوان ئەم دوو کلیلە دا، کە ناسراون بە کلیلی گشتی Public Key و، کلیلی تایبەتی یان نهێنی Private Key (OR Secret)، ئەلگۆریسمەکانی بەهێماکردنی ناهاوتا Asymmetric Encryption Algorithms، کلیلی بیرکارییانە Mathematically Key بەکاردەهێنێت کە دووانە کلیلی پەیوەندی دارن بۆ بەهێماکردن Encryption و گۆرینی بەهێماکردنەکە بۆ نووسینی ئاسایی Decryption.



ئەلگۆریسمەکانی بە هێماکردنی ناهاوتا

Asymmetric Encryption Algorithms

ئەمانەی لا ی خوارەوە گەورەترین و باوترین ئەلگۆریسمەکانی بەهێماکردنی ناهاوتان کە بەکاردەهێنرێن بۆ بەهێماکردن یان ئیمزایی ژمارەیی زانیاری Digitally Signing Data.

١. ڕێککەوتننامەی سەرەکی دیفی – هێڵمان Diffie – Hellman Key Agreement : ئەم ئەلگۆریسمە دروستکراوە لە لایەن دکتۆر یتفیلد دیفی Dr.Whitfield Diffie، و دکتۆر مارتن هیلمان Dr.Martin Hellman in 1976. ئەلگۆریسمی دیفی – هێڵمان بۆ بەهێما کردن

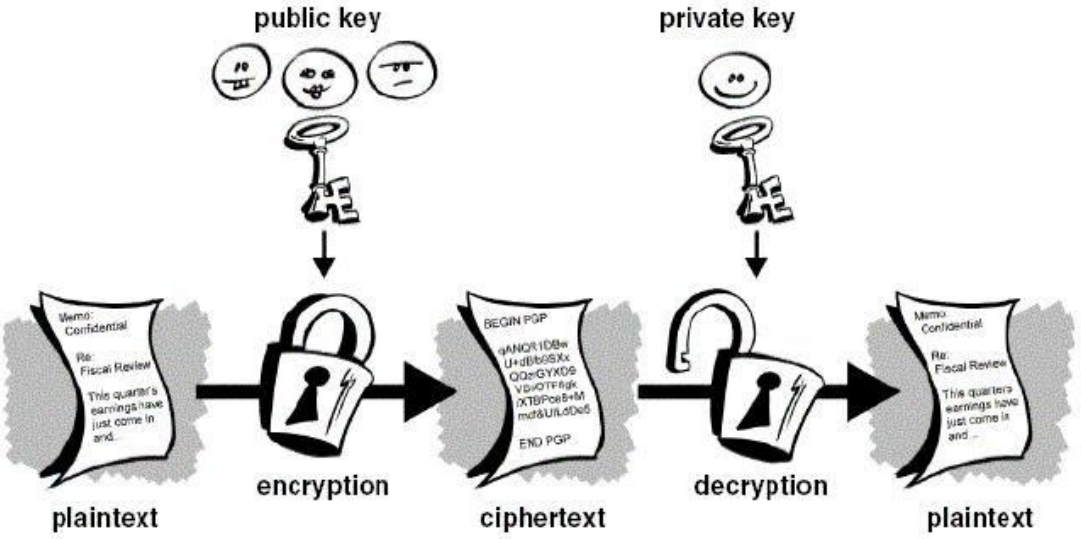
Encryption و گۆرینەوەی بەهێماکردنەکە بۆ نووسینی ئاسایی Decryption نی یە، کە لەهەردوو لاوە بەشدار دەبێت بۆ گەیاندن و دروستکردنی کلیلی نهێنی هاوبەش و بەشدار پێکراو Shared Secret Key بۆ ئالۆگۆر کردنی زانیاری نهێنی بە تەواوی و بێگرفت.

٢. ئار ئێس ئەی RSA: ئەم ئەلگۆریسمە (ئار ئیس ئەی RSA) کورتکراوەی Rivest Shamir Adlemanـە و، لەلایەن رۆن ریڤێست Ron Rivest، ئادی شامیر Adi Shamir و لێن ئادلیمانەوە Len Adleman دروستکرا و، ناوەکەی لە یەکپێگرتنی ناوی هەرسێکیان پێکهاتووە، لە ساڵی ١٩٧٨، ئەلگۆریسمی کلیلی گشتی یە، ئەم ئەلگۆریسمە بەکاردێت بۆ بەهێما کردن Encryption و ئیمزا لە سەر زانیاری Data Signing، کرداری بە هێماکردن Encryption و، ئیمزا لە سەر زانیاری Data Signing بە ئەنجام دەگات لە رێگەی زنجیرەیەك لێکدانەوە.

٣. کریپتۆ گرافی بەبەکارهێنانی چەماوەی هێلکەیی Elliptic Curve Cryptography (ECC): ئەم ئەلگۆریسمە هەمان کاری ئارِ ئێس ئەی Similar Functionality دابین دەکات، کە لە ئامێری بچووك دا بەکاردەهێنرێت، وەکو لە مۆبایل Cell Phoneدا.

٤. جەمەل El Gamal: ئەلگۆریسمێکە بەکاردەهێنرێت بۆ ئیمزایی ئەلیکترۆنی Digital Signature و ئالۆگۆریی بنچینەیی، ئەم رێگەیە لەسەر بنچینەیی ژمێرەیی لۆگاریتمە Calculating Logarithm، واتە لەسەر بنچینەی رووخسارەکانی ژمارە لۆگاریتمی یەکان و ژمێرەیی، ئەلگۆریسمی دی ئێس ئەی DSA Algorithm لەسەر بنچینەی ئەم ئەلگۆریسمەیە.

٥. ئەلگۆریسمی ئیمزای ئەلیکترۆنی Digital Signature Algorithm (DSA): ئەم ئەلگۆریسمە لەلایەن حکومەتی ویلایەتە یەکگرتووەکانی ئەمریکاوە دروستکراوە بۆ ئیمزایی ئەلیکترۆنی. ئەم ئەلگۆریسمە بەکاردەهێنرێت بۆ ئیمزاکردنی زانیاری Signing Data، بەلام بۆ بەهێماکردن Encryption بەکارناهینریت.

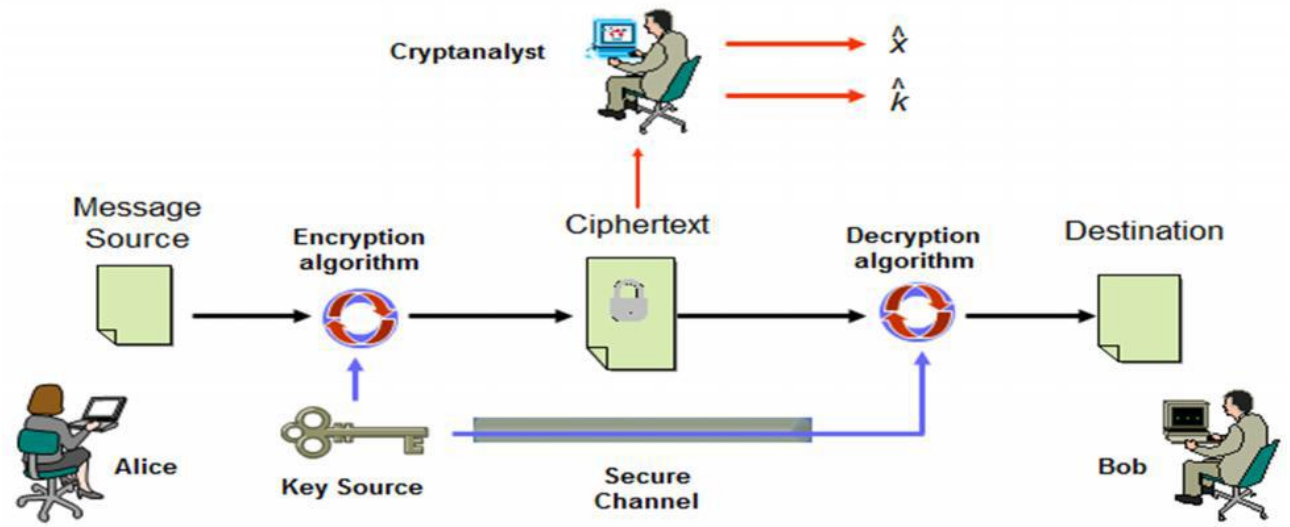


شیکار کەری کریپتۆگرافی و هێرشی سەر کریپتۆسیستەم

Ceyptanalysis and Attack on Cryptosystem

شیکار کەری کریپتۆگرافی Cryptanalysis هونەری گۆرینەوەی بەهێماکراوەکانە Encrypted بۆ نووسین و شێوەی ئاسایی Plain Text کە لێی تێبگەین و، بتوانین بیخوێنینەوە، بە بێ بوونی زانیاری لە بارەی کلیلی Key بە هێماکردنەکەوە. هەروەها دەتوانین بڵێین پرۆسەی شیکردنەوەی سیستەمە پارێزراوەکانی زانیاری یە بۆ دۆزینەوەی بەشی شاراوە،ئامانج لە شیکردنەوەی کریپتۆگرافی Cryptanalysis بریتییە لە گۆرینی زانیاری بەهێماکراو Decrypted Encrypted Data ، بەبێ زانینی کلیلی نهێنی Secrete Key.

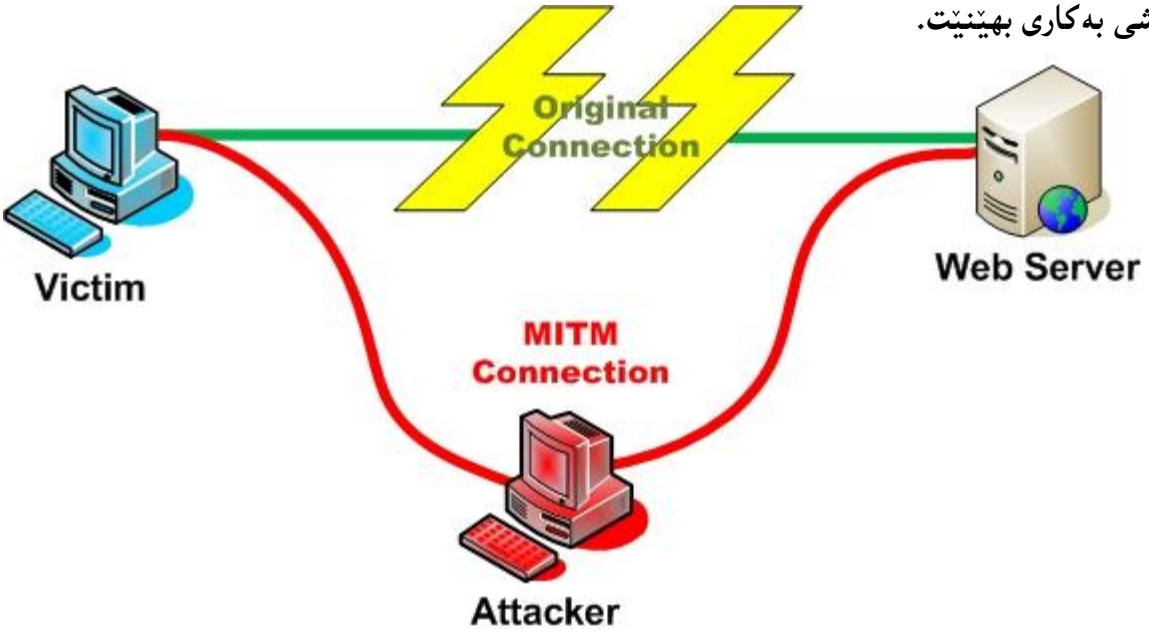
بۆ زانیاری بۆ ئەم بەستەش زۆر رێگە و تەکنیکمان هەیە کە بەکورتی باس لە گرنگترین رێگە و تەکنیکەکان دەکەین:



- **تەنها هێرش بۆ سەر نووسینی سایفەر Cipher Text – Only Attack**: لەم جۆرەدا هێرشبەر Attacker هیچ زانیارییەك نازانێت لەبارەی ناوەرۆکی نامە و پەیامەوە، پێویستە تەنها کاربکات لەسەر نووسینی بەهێماکراو Cipher Text.
- **هێرش بە زانینی نووسینی ئاسایی Known – Plain Text Attack**: لەم جۆرەدا هێرشبەر نووسینی ئاسایی Plain Text دەزانێت یان دەتوانێت بیزانێت بۆ هەندێك بەشی نووسینی سایفەر Cipher Text کە بەکاردەهێنرێت بۆ گۆرینەوەی نووسینی سایفەر بۆ نووسینی ئاسایی

Decryption، بە سوود وەرگرتن لەم زانیارییە زانراوانە.

- هێرش بەهۆی هەلبژاردنی نووسینی ئاساییەوە Chosen Plain Text Attack: جۆرێکی شیکردنەوەی کریپتۆگرافییە Cryptanalysis کە شیکار کەر Cryptanalyst نوسینێکی ئاسایی Plain Textهەلدەبژێرێت کە بەهێما کراوە to be Encrypted.
- هێرشی پیاوێك لە ناوەراست دا Man in the Middle Attack: ئەم جۆرە هێرشە پەیوەندە بە گەیاندنی کریپتۆگرافی و رێککەوتننامەی ئالۆگۆری کلیل، واتە جۆرێکی هێرشی ئەلیکترۆنی یە و، کەسێکی خراپەکار دێتە نێوان پەیوەندی و گفتووگۆی دووکەسەوە و هەوڵ دەدات زانیاری نێوانیان وەربگرێت وپاشان بینیریتەوە بۆ وەرگرە بنەرەتی یەکە و زانیارییەکەش بۆ مەبەستی دیاری کراوی خۆشی بەکاری بهێنێت.



- هێرشی فەرهەنگ Dictionar Attack:لەم جۆرەدا هێرش بەر هەوڵی بەدەست هێنانی تیپەرە وشە Password یان کلیل Key دەدات لە رێگەی لیستەیەکەوە.

بەهێماکردنی کۆن

Clasical Encryption

کریپتۆگرافی شێوازی بەکارهێنانی کۆدەکان Codes و سایفەرە Ciphers، بۆ بەهێماکردنی نامە و پەیامەکان Encrypt Message و، گۆرینی بۆ شێوەیەك کە نەخوێنرێتەوە Unreadable، و ناردنی بۆ وەرگر کە کلیلی تایبەتی لایە بۆ گێرانەوەی نووسینە هێماکە بە شێوە و نووسینی ئاسایی Decrypt، ئەم بەهێماکردنە دەگەڕێتەوە بۆ سەدان ساڵ پێش ئیستا .

یەکەم// سایفەری خستنە جێ

Substitution Cipher

لەم جۆرەی سیستەمی کریپتۆگرافی Cryptosystemدا، ئەلگۆریسمەکە خستنە جێی کارەکتەر بە کارەکتەرە بە بەکارهێنانی کلیلێك، خستنە جێکان بە پێی لیستێکی ئەلف و بێی دەبێت، کە ژمارەی پیتەکانی زمانی ئینگلیزی تەنها ٢٦ پیتە.

١. سایفەری یەك ئەلف و بێی Mono Alphabetic Cipher: لەم جۆرەی بەهێما کردن دا، پیتێك دەخرێتە جێی پیتێکی تر، بۆ نموونە ئەی پیتی کەی لە جیاتی دادەنرێت، لە بەهێما کردن دا. نموونەی ئەم جۆرە سایفەرە وەکو ئەمانەی لای خوارەوە.

- سیزەر سایفەر Caesar Cipher.
- سایفەری پێوەری پێچەوانە Standard Reverse Cipher.
- سایفەری لێکدان Multiplicative Cipher.
- سایفەری ئەفاین Affine Cipher.
- سایفەری ئەلفبێی تێکەلاو Mixed Alphabet Cipher.
- ئەتباش سایفەر Atbash Cipher.
- سایفەری وشەی تێکەڵاو Keyword Mixed Cipher.
- سایفەری وشە گواستنەوەی تیکەلاو Transposed Keyword Mixed Cipher.
- سایفەری بیلڕ Beal Cipher.
- سایفەری ریکخستنی بەرز Higher Order Cipher.

- پێکپێن/ماسۆنیك سایفەر Pigpen/Masonic Cipher.
- پۆلیباس Polybius Square.

٢. سایفەری فرە ئەلف و بێی Poly Alphabetic Cipher: لە سایفەری فرە ئەلف و بێی Poly Alphsbetic Cipher دا، خستنەجێی لەوانەیە لە رێگەی نامە و پەیامێکەوە بێت، بۆ نموونە پیتی ئەی A لە بەشێکە نامە و پەیامەکەدا ببێت بە کەی k، بەلام لە بەشێکی تری نامە و پەیامەکەدا پیتی ئەی A ببێت بە دەبلیوو W. نموونەی ئەم جۆرە سایفەرە وەکو :

- ڤیجنێر سایفەر Vigener Cipher.
- سایفەری بیوفۆرت Beaufort Cipher.
- سایفەری ئۆتۆکی Auto Key Cipher.
- سایفەری رەنینگ کی Running Key Cipher.

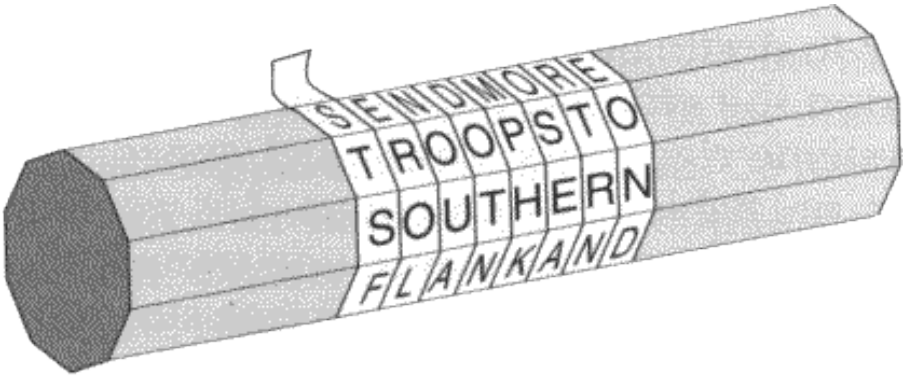
٣. سایفەر ی پۆلیگرافیك Polygraphic Cipher: لە جیاتی خستنەجێی پیتێك بۆ پیتێکی تر، سایفەری پۆلیگرافیك جیبەجێکردنی خستنە جێیەکانە لەگەڵ دوو یان زیاتری کۆمەلێك لە پیتەکان، وەکو ئەمانەی لای خوارەوە:

- سایفەری پلەی فایەر Play Fair Cipher.
- سایفەری بیفید Bifid Cipher.
- سایفەری ترافید Trifid Cipher.
- سایفەری چوار – چوار لا Four – Square Cipher.
- سایفەری هیلّ Hill Cipher.

دووەم// سایفەری جیگۆرکی

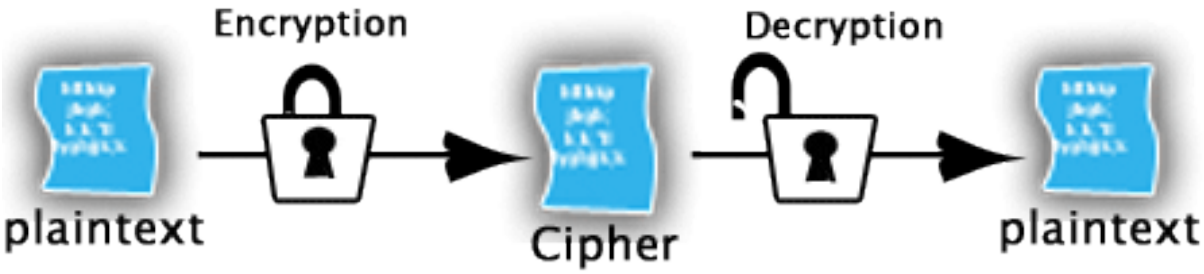
Transposition Cipher

لە کریپتۆ گرافی Cryptographyدا، سایفەری جیگۆرکیّ تەنها گۆرینی شوینی پیتەکانە و لەکاتیکدا جۆری پیشتر Substitution Cipher بریتی بوو لە لەجیاتی دانان و جیگرتنەوەی پیتەکان بە پیتی تر.



ئەم جۆرە بە پێچەوانەی جۆری خستنە جێوە Substitution Cipher لە جۆری سایفەری دارِشتگە و قالّبە Template، نموونەی جۆری سایفەری جێگۆرکێ وەکو ئەمانەی لای خوارەوە:

- سایفەری رێگە Route Cipher.
- سایفەری رەیل فینس Rail Fence Cipher.
- سایفەری ئالۆگۆری ستوونی Columnar Transposition Cipher.
- سایفەری ئالۆگۆری دووانی Double Transposition Cipher .
- ئالۆگۆری میسکاوسکی Myszkowski Transposition.



ئەلگۆریسمەکان

Algorithms

سایفەری یەك ئەلف و بێی و سایفەری فرە ئەلف و بێی و سایفەری پۆلیگرافیك ، ئەلگۆریسمیان زۆرە و نموونەیان بۆ ئەهینینەوە بە گویرەی پێویست شییان ئەکەینەوە.

سایفەری سیزەر

Caesar Cipher

سایفەری سیزەر Caesar Cipherیەکێکە لە سادەترین رێگەکانی بەهێماکردن Encryption Methods، کە سایفەری خستنە جێیە و، هەرپیتیکی نووسینە ئاساییەکە Plain Textدەگۆردرێت بە پیتێکی تر بۆ درووستکردنی بەهێماکراو Encrypted، بە بەکارهێنانی یاسا و رێسایی تایبەتی.

بۆ بەهێماکردن Encryption ئەم یاسایەی لای خوارەوە بەکاردەهینرێت:

Cipher Text (C)=Plain Text (P)+Key Mod 26

C=p+k%26

بەلام بۆ پێچەوانە کردنەوە و گۆرینی بە هێماکراو Encrypted بۆ نووسینی ئاسایی Plain Text ئەم یاسایە بەکاردەهێنین:

Plain Text (P)=Cipher Text (C) – Key (K) Mod 26

پرسیاری یەکەم: بە بەکارهێنانی ئەلگۆریسمی سیزەر سایفەر Caesar Cipher ئەم ناوەی خوارەوە بگۆرە بۆ ناوێکی ناروون کە لێی تێنەگەین Cipher، و نەخوێندرێتەوە، واتە بیکە بە کۆد Encryption، بە بەکارهێنانی ۳ وەك کلیلی گۆرینەکە:

Hemn Barznji

وەلآم:

یەکەم// سەرەتا لە خشتەیەك دا، پیتەکانی زمانی ئینگلیزی دەنووسین و ژمارەیان بۆ دادەنێین لە سفر بۆ ۲۵:

z	Y	x	w	v	u	t	s	r	q	p	o	n	m	l	k	j	i	h	g	f	e	d	c	b	a
25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0

دووەم// ئەم یاسایەی خوارەوە بەکاردەهێنرێت بۆ مەبەستی Encryption

Cipher Text (C)=Plain Text (P)+Key Mod 26

C=p+k%26

سێهەم: یاساکە بۆ هەریەکێك لە پیتەکانی ناوەکە جێبەجێبکە، بەم جۆرەی لای خوارەوە:

$C_h=P_h+k\%26=7+3\%26=10\%26=10=k$

$C_e=P_e+K\%26=4+3\%26=7\%26=7=h$

$C_m=P_m+K\%26=12+3\%26=15\%26=15=p$

$C_n=P_n+K\%26=13+3\%26=16\%26=16=q$

بەمەش ناوی hemn بوو بە khpq، ئیستا هەنگاوەکانی سەرەوە بۆ ناوی دووەم، barznji جێبەجێدەکەین:

$C_b=P_b+K\%26=1+3\%26=4\%26=4=e$

$C_a=P_a+K\%26=0+3\%26=3\%26=3=d$

$C_r=P_r+K\%26=17+3\%26=20\%26=20=u$

$C_z=P_z+K\%26=25+3\%26=28\%26=2=c$

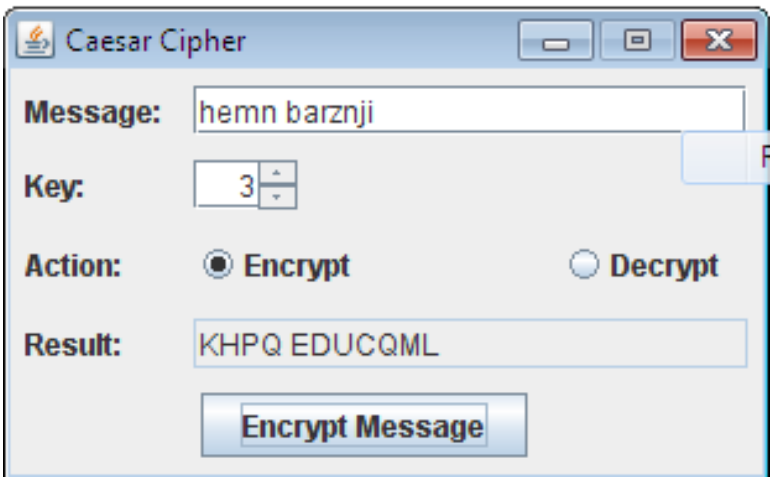
$C_n=P_n+K\%26=13+3\%26=16\%26=16=q$

$C_j=P_j+K\%26=9+3\%26=12\%26=12=m$

$C_i=P_i+K\%26=8+3\%26=11\%26=11=l$

بەمەش ئەنجامی گۆرینەکەی وشەی دووەم کە barznjiبوو، بووبە educqml.

گۆرینی هەردوو وشەکە بوو بە : khpq educqml واتە ئەنجامی کۆتایی ئینکرپیشنەکەیە.



پرسیاری دووەم: ئەم وشە بە کۆدکراوانەی Cipher لای خوارەوە بگۆڕەوە Decrypt بۆ وشە و ناوێکی ئاسایی کە بخوێنرێتەوە و لێی تێبگەین، بە بەکارهێنانی کلیلی ژمارە ٣...؟؟

وەڵام:

یەکەم: سەرەتا لە خشتەیەك دا، پیتەکانی زمانی ئینگلیزی دەنووسین و ژمارەیان بۆ دادەنێین لە سفر بۆ ٢٥:

z	Y	x	w	v	u	t	s	r	q	p	o	n	m	l	k	j	i	h	g	f	e	d	c	b	a
25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0

دووەم// ئەم یاسایەی خوارەوە بەکاردەهێنرێت بۆ مەبەستی Decryption ناوەکان:

Plain Text (P)=Cipher Text (C) – Key (K) Mod 26

سێهەم: یاساکە بۆ هەریەکێك لە پیتەکانی ناوەکە جێبەجێبکە، بەم جۆرەی لای خوارەوە:

$P_k=C_k-K\%26=10-3\%26=7\%26=7=h$

$P_h=C_h-K\%26=7-3\%26=4\%26=4=e$

$P_p=C_p-K\%26=15-3\%26=12\%26=12=m$

$P_q=C_q-K\%26=16-3\%26=13\%26=13=n$

بەم هەنگاوانە توانیمان پیتەکانی khpq بگۆڕین بۆ وشەیەك کە مانا دەدات و بریتییە لە ناوی هێمن hemn. ئیستا پیتەکانی educqml بگۆڕە بۆ ناوێك کە دەخوێنرێتەوە و مانادەدات و، شاراوە نییە، بە بەکارهێنانی هەنگاوەکانی پێشوو، بەم شێوەیە:

$Pe_=C_e-K\%26=4-3\%26=1\%26=1=b$

$P_d=C_d-K\%26=3-3\%26=0\%26=0=a$

$P_u=C_u-K\%26=20-3\%26=17\%26=17=r$

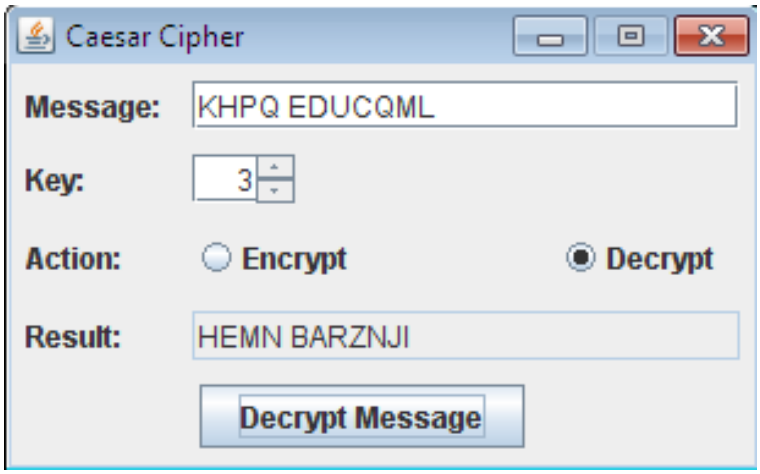
$P_c=C_c-K\%26=2-3\%26=-1\%26=25=z$

$P_q=C_q-K\%26=16-3\%26=13\%26=13=n$

$P_m=C_m-K\%26=12-3\%26=9\%26=9=j$

$P_l=C_l-K\%26=11-3\%26=8\%26=8=i$

بەمەش وشەی دووەمان گۆڕییەوە Decrypt بۆ ئەو ناوەی کە روونە و دەخوێنرێتەوە، واتە educqml بوو بە barznji



پرسیار سێهەم: بەشێوەی هەنگاو و بە هەنگاو ئەم دوو وشەیەی لای خوارەوە بکە بە هێما Encrypt، بە بەکارهێنانی ئەلگۆریسمی سیزەر سایفەر Caesar Cipher، ژمارە ((٥)) بەکاربهێنە وەکو کلیل Key، هەموو هەنگاوەکان بنووسە لە یەکەم هەنگاو تا کۆتا هەنگاو.

Zankoy Slemani

وەڵام://

یەکەم// سەرەتا لە خشتەیەك دا، پیتەکانی زمانی ئینگلیزی دەنووسین و ژمارەیان بۆ دادەنێین لە سفر بۆ ٢٥:

z	Y	x	w	v	u	t	s	r	q	p	o	n	m	l	k	j	i	h	g	f	e	d	c	b	a
25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0

دووەم// ئەم یاسایەی خوارەوە بەکاردەهێنرێت بۆ مەبەستی Encryption

Cipher Text (C)=Plain Text (P)+Key Mod 26

C=p+k%26

سێهەم: یاساکە بۆ هەریەکێك لە پیتەکانی ناوەکە جێبەجێبکە، بەم جۆرەی لای خوارەوە:

$C_z=P_z+k\%26=25+5\ \%\ 26=30\ \%\ 26=4=e.$

$C_a=P_a+K\%26=0+5\ \%\ 26=5\ \%\ 26=5=f.$

$C_n=P_n+K\%26=13+5\ \%\ 26=18\ \%\ 26=18=s.$

$C_k=P_k+K\%26=10+5\ \%\ 26=15\ \%\ 26=15=p.$

$C_o=P_k+K\%26=14+5\ \%\ 26=19\ \%\ 26=19=t.$

$C_y=P_k+K\%26=24+5\ \%\ 26=29\ \%\ 26=3=d.$

بەمەش ناوی zankoy **بوو بە** efsptd**، ئیستا هەنگاوەکانی سەرەوە بۆ ناوی دووەم،** slemani

جێبەجێدەکەین:

$C_s=P_s+K\%26=18 + 5 \% 26 = 23 \% 26 =23 = x.$

$C_l=P_e+K\%26=11+5 \% 26 = 16 \% 26 = 16 = q.$

$C_e=P_e+K\%26=4 + 5 \% 26 = 9 \% 26 = 9 = j.$

$C_m=P_m+K\%26=12+ 5 \% 26 = 17 \% 26 = 17 = r.$

$C_a=P_a+K\%26=0 + 5 \% 26 = 5 \% 26 = 5 = f.$

$C_n=P_n+K\%26=13+ 5 \% 26 = 18 \% 26 = 18 = s.$

$C_i=P_i+K\%26=8+ 5 \% 26=13 \% 26= 13 = n.$

بەمەش ئەنجامی گۆرینەکەی وشەی دووەم کە slemaniبوو، بووبە xqjrfsn.

گۆرینی هەردوو وشەکە بوو بە : efsptd xqjrfsn واتە ئەنجامی کۆتایی ئینکرپیشنەکەیە.

پرسیاری چوارەم: هەنگاو بەهەنگاو ئەم دوو سایفەرەی خوارەوە بگۆڕەوە بۆ شێوەی ئاسایی Decrypt ، بە ئەلگۆریسمی سیزەر سایفەر و کلیلی ژمارە ((٥))، هەموو هەنگاوەکان بنووسە لە یەکەم هەنگا و تا کۆتا هەنگاو.

ZUXFQF ZSNAJWXNYD

وەڵام//

یەکەم: سەرەتا لە خشتەیەك دا، پیتەکانی زمانی ئینگلیزی دەنووسین و ژمارەیان بۆ دادەنێین لە سفر بۆ ٢٥:

z	Y	x	w	v	u	t	s	r	q	p	o	n	m	l	k	j	i	h	g	f	e	d	c	b	a
25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0

دووەم// ئەم یاسایەی خوارەوە بەکاردەهێنرێت بۆ مەبەستی Decryption ناوەکان:

Plain Text (P)=Cipher Text (C) – Key (K) Mod 26

سێهەم: یاساکە بۆ هەریەکێك لە پیتەکانی ناوەکە جێبەجێبکە(ZUXFQF)، بەم جۆرەی لای خوارەوە:

$P_z=C_z-K\%26=25-5\%26=20\%26=20=u$

$P_u=C_u-K\%26=20-5\%26=15\%26=15=p$

$P_x=C_x-K\%26=23-5\%26=18\%26=18=s$

$P_f=C_f-K\%26=5-5\%26=0\%26=0=a$

$P_q=C_q-K\%26=16-5\%26=11\%26=11=l$

$P_f=C_f-K\%26=5-5\%26=0\%26=0=a$

بەم هەنگاوانە توانیمان پیتەکانی ZUXFQF بگۆرین بۆ وشەیەك کە مانا دەدات و بریتییە لە ناوی ئوپسالا upsala. ئیستا پیتەکانی ZSNAJWXNYD بگۆرە بۆ ناوێك کە دەخوێنریتەوە و مانادەدات و، شاراوە نییە، بە بەکارهێنانی هەنگاوەکانی پێشوو، بەم شێوەیە:

$Pz_=C_z-K\%26=25-5\%26=20=u.$

$P_s=C_s-K\%26=18-5\%26=13\%26=13=n$

$P_n=C_n-K\%26=13-5\%26=8\%26=8=i$

$P_a=C_a-K\%26=0-5\%26=-5\%26=21=v$

$P_j=C_j-K\%26=9-5\%26=4\%26=4=e$

$P_w=C_w-K\%26=22-5\%26=17\%26=17=r$

$P_x=C_x-K\%26=23-5\%26=18\%26=18=s$

$P_n=C_x-K\%26=13-5\%26=8\%26=8=i$

$P_y=C_x-K\%26=24-5\%26=19\%26=19=t$

$P_d=C_x-K\%26=3-5\%26=-2\%26=24=y$

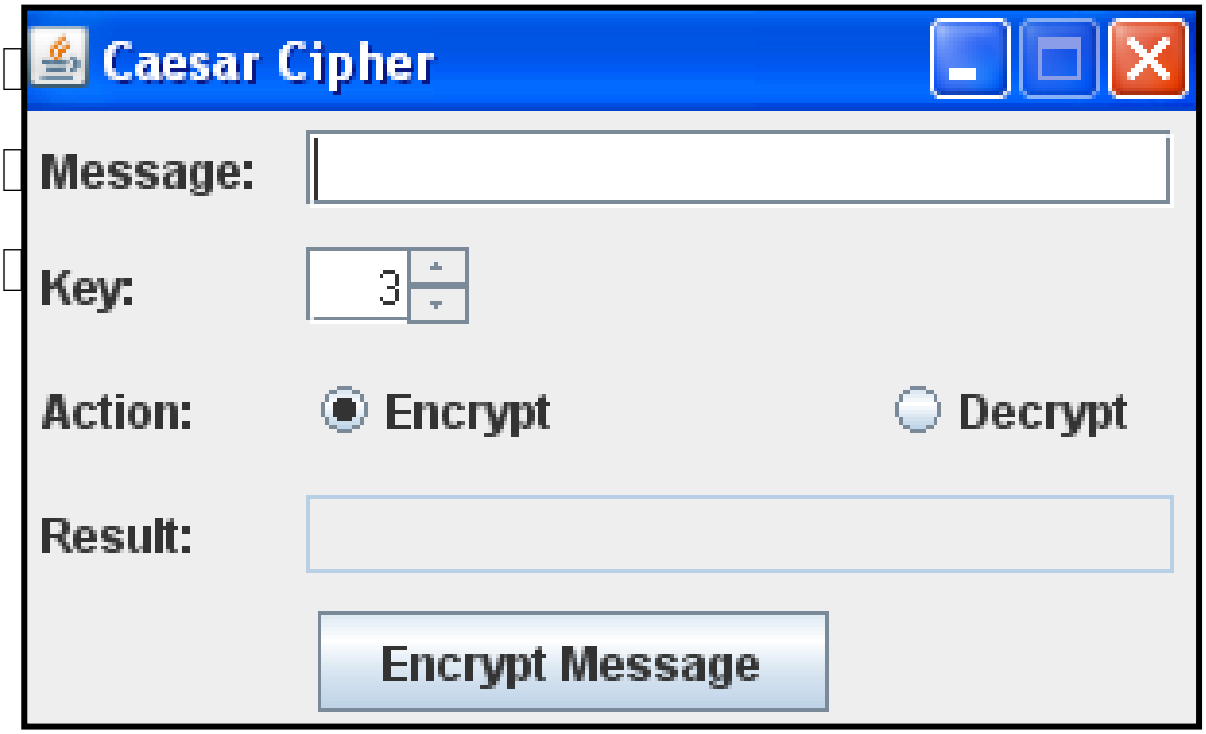
بەمەش وشەی دووەمان گۆرییەوە Decrypt بۆ ئەو ناوەی کە روونە و دەخوێنرێتەوە، واتە بوو بە university

پرسیاری پێنجەم: بە زمانی بەرنامە سازیی جاڤا، بەرنامەیەك بنووسە بۆ گۆرینی نووسینی ئاسایی Plain Text بۆ هێما Cipher و، پێچەوانە کردنەوەی ؟

```
/*

 * CaesarCipher.java
 * Encrypts/Decrypts text using the Caesar Cipher method
 * by Hemn Mela Kerym Barznji
 */

import javax.swing.*;
import java.awt.*;
import java.awt.event.*;

public class CaesarCipher extends JFrame implements ActionListener {

   private static JLabel      msgLabel      = new JLabel("Message: ");
   private static JLabel      keyLabel      = new JLabel("Key: ");
   private static JLabel      actionLabel   = new JLabel("Action: ");
   private static JLabel      resultLabel   = new JLabel("Result: ");
   private static JTextField  msgTextField  = new JTextField(20);
   private static JTextField  resultTextField = new JTextField(20);
   private static JSpinner    keySpinner    = new JSpinner( new
SpinnerNumberModel(3, 1, 25, 1) );
   private static JRadioButton encryptRadio  = new
JRadioButton("Encrypt");
   private static JRadioButton decryptRadio  = new
JRadioButton("Decrypt");
   private static JButton     actionButton   = new JButton("Encrypt
Message");
   private static JPanel      panel         = new JPanel();
   private static ButtonGroup group         = new ButtonGroup();

   public static void main(String[] args) {
      new CaesarCipher();
   }

   public CaesarCipher() {
      this.setSize(310, 192);
      this.setTitle("Caesar Cipher");
      this.setLocationRelativeTo(null);
      this.setDefaultCloseOperation(EXIT_ON_CLOSE);
      this.setResizable(false);

      panel.setLayout(new GridBagLayout());

      addComponent(panel, msgLabel, 0, 0, 1, 1,
```

```
GridBagConstraints.LINE_START);
        addComponent(panel, msgTextField, 1, 0, 2, 1,
GridBagConstraints.LINE_START);

        addComponent(panel, keyLabel, 0, 1, 1, 1,
GridBagConstraints.LINE_START);
        addComponent(panel, keySpinner, 1, 1, 1, 1,
GridBagConstraints.LINE_START);

        addComponent(panel, actionLabel, 0, 2, 1, 1,
GridBagConstraints.LINE_START);
        group.add(encryptRadio);
        group.add(decryptRadio);
        addComponent(panel, encryptRadio, 1, 2, 1, 1,
GridBagConstraints.LINE_START);
        addComponent(panel, decryptRadio, 2, 2, 1, 1,
GridBagConstraints.LINE_START);
        encryptRadio.setSelected(true);
        encryptRadio.addActionListener(this);
        decryptRadio.addActionListener(this);

        addComponent(panel, resultLabel, 0, 3, 1, 1,
GridBagConstraints.LINE_START);
        addComponent(panel, resultTextField, 1, 3, 2, 1,
GridBagConstraints.LINE_START);
        resultTextField.setEditable(false);

        addComponent(panel, actionButton, 1, 4, 1, 1,
GridBagConstraints.CENTER);
        actionButton.addActionListener(this);

        this.add(panel);
        this.setVisible(true);
    }

    private void addComponent(JPanel p, JComponent c, int x, int y, int width,
int height, int align) {
        GridBagConstraints gc = new GridBagConstraints();
        gc.gridx = x;
        gc.gridy = y;
        gc.gridwidth = width;
        gc.gridheight = height;
        gc.weightx = 100.0;
        gc.weighty = 100.0;
        gc.insets = new Insets(5, 5, 5, 5);
        gc.anchor = align;
        gc.fill = GridBagConstraints.NONE;
        p.add(c, gc);
    }
```

```
    private void encryptMessage(String msg, int k) {
        String result = "";
        resultTextField.setText("");
        for (int i = 0; i < msg.length(); i++)
            result += encryptChar(msg.charAt(i), k);
        resultTextField.setText(result);
    }

    private char encryptChar(char c, int k) {
        if (Character.isLetter(c))
            return (char) ('A' + (c - 'A' + k) % 26);
        else
            return c;
    }

    public void actionPerformed(ActionEvent e) {
        if (e.getSource() == encryptRadio)
            actionButton.setText("Encrypt Message");

        if (e.getSource() == decryptRadio)
            actionButton.setText("Decrypt Message");

        if (e.getSource() == actionButton) {
            String str = msgTextField.getText();
            int k = (Integer) keySpinner.getValue();
            int key = 0;
            String message = "";

            if (str.equals("")) {
                JOptionPane.showMessageDialog(null, "Please enter a
message!", "Error!", JOptionPane.ERROR_MESSAGE);
                msgTextField.requestFocus();
                return;
            }

            message = str.toUpperCase();
            if (encryptRadio.isSelected())
                key = k;
            else
                key = 26 - k;

            encryptMessage(message, key);
        }
    }
}
```



پرسیاری شەشەم: بەزمانی بەرنامە سازیی جاڤا Java Programming Language بەرنامەیەك بنووسە بۆ پێچەوانە کردنەوەی Decrypt، وشەئاساییەکانی Zanki Slemani کە کراوەتە کۆد ((هێما)):

```
//By: Hemn Mk. Barznji _________ Cipher_To_Plain_Caser

class Cipher_To_Plain_Caser{

   int i, z,l, k=5,cS,cC,cNs,cNc;

String ci="efsptd xqjrfsn";

char []ar={'A','B','C','D','E','F','G','H','I','J','K','L','M',

 'N','O','P','Q','R','S','T','U','V','W','X','Y','Z'};

char []arS={'a','b','c','d','e','f','g','h','i','j','k','l','m',
'n','o','p','q','r','s','t','u','v','w','x','y','z'};


char []pla=ci.toCharArray();

void m(){

char []ar2=new char[pla.length];
```

```
for( z=0;z<pla.length;z++){
for(i=0;i<ar.length;i++){
cC=(i-k)%26;
if(pla[z]==ar[i]&&cC>=0){
  i=cC;
  ar2[z]=ar[i];
break;
}
else{
ar2[z]=pla[z];
}
//////////////////
cNc=(i-k)%26;
if(pla[z]==ar[i]&&cC<0){
cNc=cNc+26;
  i=cNc;
  ar2[z]=ar[i];
 break;
}
else{
}
}
for(l=0;l<arS.length;l++){
```

```
cS=(l-k)%26;
if(pla[z]==arS[l]&&cS>=0){
  l=cS;
ar2[z]=arS[l];
   break;
}
else{
}
cNs=(l-k)%26;
if(pla[z]==arS[l]&&cNs<0){
cNs=cNs+26;
  l=cNs;
 ar2[z]=arS[l];
   break;
}
else{
}
}
}
String s= new String(ar2);
System.out.println(" "+s);
}
public static void main (String[] args){
```

```
Cipher_To_Plain_Caser ob=new Cipher_To_Plain_Caser();
ob.m();
}
}
```

پرسیاری شەشەم: بەزمانی بەرنامە سازیی جاڤا Java Programming Language بەرنامەیەك بنووسە بۆ بەهێماکردنی زانیاری Encryption و بۆ گۆڕینی نووسینی ئاسایی Plain Text بۆ هێما Cipher.

```
//Hemn Mk. Barznji _________ Plaintext_To_Ciphertext_Caser
import java.util.*;
class Plaintext_To_Ciphertext_Caser{
Scanner sc = new Scanner(System.in);
   int i, z,l,cS,cC,cNs,cNc;
         String ci="Upsala University";
char []ar={'A','B','C','D','E','F','G','H','I','J','K','L','M', 'N','O','P','Q','R','S','T','U','V','W','X','Y','Z'};

char []arS={'a','b','c','d','e','f','g','h','i','j','k','l','m', 'n','o','p','q','r','s','t','u','v','w','x','y','z'};
char []pla=ci.toCharArray();
void m(){
         System.out.println("Please Enter key = ");
int k=sc.nextInt();
char []ar2=new char[pla.length];
for( z=0;z<pla.length;z++){
for(i=0;i<ar.length;i++){
cC=(i+k)%26;
if(pla[z]==ar[i]){
```

```
            i=cC;
            ar2[z]=ar[i];
break;
}
else{
          ar2[z]=pla[z];
}
}
//////////////////
for(l=0;l<arS.length;l++){
          cS=(l+k)%26;
if(pla[z]==arS[l]){
                    l=cS;
                    ar2[z]=arS[l];
  break;    }
else{   }   }   }
String s= new String(ar2);
System.out.println(" "+s);   }
public static void main (String[] args){
Plaintext_To_Ciphertext_Caser ob=new Plaintext_To_Ciphertext_Caser();
ob.m();
}
}
```

سایفەری پێچەوانە

Reverse Cipher

سایفەری پێچەوانە یەکێکە لەو ڕێگایانەی کە پێتەکانی ئەلف و بێ ی Alphabetic Letters پێچەوانەیە و، لە زێت Z بۆ ئەی A ڕیزکراوە، واتە ئەی A ئالۆگۆڕ بووە Swapped بۆ زیت Z و، بی Bئالۆووگۆڕ بووە بۆ وای Y و بەو شێوەیە.

٠	١	٢	٣	٤	٥	٦	٧	٨	٩	١٠	١١	١٢	١٣	١٤	١٥	١٦	١٧	١٨	١٩	٢٠	٢١	٢٢	٢٣	٢٤	٢٥
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	Q	Y	Z
25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
Z	Y	Q	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A

بۆ ئەنجامدانی گۆڕینی نووسینێکی ئاسایی Plain Text بۆ سایفەر Cipher Text ئەم یاسایی لای خوارەوە بەکاردەهێنین:

Cipher Text (CT) = (25 – Plain Text (M) + Key) Mod 26=(25-M+k)Mod26

بۆنمونە ئەگەر کلیلەکە Key یەکسانبێت بە سفر ((•))، بۆ گۆڕینی نووسینێکی ئاسایی Plain Text کە بریتییە لە University، ئەوا بە بەکارهێنانی یاساکەی سەرەوە ئەم هەنگاوانە جێبەجێدەکەین:

C_u=(25-P_u+Key)Mod26=(25-20+0)%26=5%26=5=F.

C_n=(25-P_n+Key)Mod26=(25-13+0)%26=12%26=12=M.

C_i=(25-P_i+Key)Mod26=(25-8+0)%26=17%26=17=R.

C_v=(25-P_v+Key)Mod26=(25-21+0)%26=4%26=4=E.

C_e=(25-P_e+Key)Mod26=(25-4+0)%26=21%26=21=V.

C_r=(25-P_r+Key)Mod26=(25-17+0)%26=8%26=8=I.

C_s=(25-P_s+Key)Mod26=(25-18+0)%26=7%26=7=H.

C_i=(25-P_i+Key)Mod26=(25-8+0)%26=17%26=17=R.

C_t=(25-P_t+Key)Mod26=(25-19+0)%26=6%26=6=G.

C_y=(25-P_y+Key)Mod26=(25-24+0)%26=1%26=1=B

ئەنجامی گۆڕینەکە و، ئەو سایفەرەی دروستبووە بریتییە لەمەی خوارەوە:

Cipher Text= FMREVIHRGB

گۆڕینی سایفەر بۆ نووسینی ئاسایی

Decryption of Standard Reverse

بۆ ئەوەی نووسینیکی سایفەر Cipher Text بگۆڕین بۆ نووسینی ئاسایی Plain text، ئەوا ئەم یاسایە بەکار دەهێنین :

Plain Text (i) = (25-Cipher Text (i)) Mod26

P_i= (25-C_i) Mod26

بۆ نموونە ئەگەر بمانەوێت ئەنجامی گۆڕینی نووسینە ئاساییەکەی پێشوو بگۆڕینەوە بۆ نووسینە ئاساییەکە Plain Text:

Cipher Text= FMREVIHRGB

ئەم هەنگاوانەی لای خوارەوە جێبەجێدەکەین:

١. پیتەکانی زمانی ئینگلیزی لە خشتەیەکدا دادەنێین:

٠	١	٢	٣	٤	٥	٦	٧	٨	٩	١٠	١١	١٢	١٣	١٤	١٥	١٦	١٧	١٨	١٩	٢٠	٢١	٢٢	٢٣	٢٤	٢٥
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	Q	Y	Z
25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
Z	Y	Q	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A

٢. ئەم یاسایە بەکار دەهێنین:

Plain Text (i) = (25-Cipher Text (i)) Mod26

P_i= (25-C_i) Mod26

٣. یاساکە بۆ هەر یەکیك لە پیتەکان جیبەجیدەکەین :

Cipher Text= FMREVIHRGB

P_F= (25-C_F) Mod26= (25-5) Mod26=20Mode26=20=U

P_M= (25-C_M) Mod26= (25-12) Mod 26= 13 Mod 26=13=N

P_R= (25-C_R) Mod26= (25-17)Mod26= 8 Mod 26=8= I

P_E= (25-C_i) Mod26=(25-4)mod26=21mod26=21=V

P_V= (25-C_i) Mod26=(25-21)mod26=4mod26=4=E

P_I= (25-C_i) Mod26=(25-8)mod26=17mod26=17=R

P_H= (25-C_i) Mod26=(25-7)mod26=18mod26=18=S

P_R= (25-C_i) Mod26=(25-17)mod26=8mod26=8=I

P_G= (25-C_i) Mod26=(25-6)mod26=19mod26=19=T

P_B= (25-C_i) Mod26=(25-1)mod26=24mod26=24=Y

Plain Text = University

بەرنامەیەك بنووسە بۆ گۆڕینی نووسینی ئاسایی بۆ هێما

کۆدی Encryption **ی سایفەری پێچەوانە:**

```
//By: Hemn Mk. Barznji _________ Cipher_Stander_revers
class Stander_revers{
   int i, z,l, k=0,cS,cC,cNs,cNc;
        String ci="university";
char []ar={'A','B','C','D','E','F','G','H','I','J','K','L','M',
'N','O','P','Q','R','S','T','U','V','W','X','Y','Z'};
char []arS={'a','b','c','d','e','f','g','h','i','j','k','l','m',
         'n','o','p','q','r','s','t','u','v','w','x','y','z'};
char []pla=ci.toCharArray();
void m(){
char []ar2=new char[pla.length];
for( z=0;z<pla.length;z++){
for(i=0;i<ar.length;i++){
cC=(25-i+k)%26;
if(pla[z]==ar[i]&&cC>=0){
          i=cC;
          ar2[z]=ar[i];
break;}
else{
        ar2[z]=pla[z];
}
```

```
//////////////////
cNc=(25-i+k)%26;
if(pla[z]==ar[i]&&cC<0){
        cNc=cNc+26;
         i=cNc;
         ar2[z]=ar[i];
 break;
}
else{
}
}
for(l=0;l<arS.length;l++){
        cS=(25-l+k)%26;
if(pla[z]==arS[l]&&cS>=0){
                l=cS;
                ar2[z]=arS[l];
  break;
}
else{
}
cNs=(25-l+k)%26;
if(pla[z]==arS[l]&&cNs<0){
                cNs=cNs+26;
```

```
                    l=cNs;
                    ar2[z]=arS[l];
  break;   }
else{   }   }   }
String s= new String(ar2);
System.out.println(" "+s);
}
public static void main (String[] args){
Stander_revers ob=new Stander_revers();
ob.m();
}
}
```

سایفەری لێکدان

Multiplicative Cipher

ئەم جۆرەی کریپتۆگرافی پشت دەبەستێت بە لێکدانی Multiply هەر کارەکتەرێك Each Character لە کلیلێك Key کە نرخێکی دیاری کراوی هەیە.

بە بەکارهێنانی ئەم یاسایە کارەکە ئەنجام دەدرێت E(M) = (Plain Text (P) * Key) Mod 26 کاتێك کلیل Key و 26 کە پەیوەندییەکی بنچینەی تایبەت بە ژمارەی خۆبەش Relatively Prime هەیە لە نێوانیان دا و، بە (BCD(K, 26) = 1) ناودەبرێت.واتە پێکەوە بەسەر یەك (١) دا، دابەش دەبن. هەروەها پێویستە کلیلەکە یەکسانبێت بە ژمارەیەکی تاك Odd Number و، یەکسان نەبێت بە (١٣).

Cipher Strip

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

نمونەی ١:

بە بەکارهێنانی ئەلگۆریسمی لێکدان Multiplicative Cipher Algorithm وشەی کۆمپیوتەر Computer بگۆڕە بۆ وشەیەك کە نەخوێندرێتەوە و بیکە بە کۆد Encryption، ئەگەر کلیلەکە The Key بریتیبێت لە ٣.

وەڵام:

١. سەرەتا پیتەکانی زمانی ئینگلیزی لە خشتەیەك دا، دەنووسین:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

٢. یاسای سایفەری لێکدان Multiplicative Cipher کە بریتییە لە E(M)=P*K Mod 26 بەکاردەهێنین.

٣. یاساکە بەسەر هەریەکێك لە پیتەکانی وشەی Computerدا، جێبەجێدەکەین، بەم جۆرەی لای خوارەوە:

- E (c) =P*k Mod 26 = 2*3%26=6%26=6 (g).
- E (o) =P*k Mod 26 =14*3%26=42%26=16 (q).
- E (m) =P*k Mod 26 =12*3%26=36%26=10 (k).
- E (p) =P*k Mod 26 =15*3%26=45%26=19 (t).
- E (u) =P*k Mod 26 =20*3%26=60%26=8 (i).
- E (t) =P*k Mod 26 =19*3%26=57%26=5 (f).
- E (e) =P*k Mod 26 =4*3%26=12%26=12 (m).
- E (r) =P*k Mod 26 =17*3%26=51%26=25 (z).

٤. ئەنجامی کۆتایی بەم شێوەیەیە، و وشەی کۆمپیوتەر Computer بووبە:

Cipher (c) = gqktifmz

ئەگەر لەو نمونەیەدا، کلیلێك هەلنەبژێرین کە بگونجێت و لەگەڵ ٢٦ دا، بکاتە ١، واتە GCD (k, 26)=1 جیبەجێنەبێت، ئەوا ئەنجامەکە هەڵەی دەبێت و، کارەکەمان دروست نابێت، بۆ نمونە ئەگەر کلیلی ژمارە (٤) Key هەلبژێرین و، هەمان نمونەکەی پێشووی پێ تەشفیر بکەین، واتە وشەی کۆمپیوتەر Computer:

- E (c) =P*k Mod 26 = 2*٤%26=٨%26=٨ (i).
- E (o) =P*k Mod 26 =14*٤%26=56%26=4 (e).
- E (m) =P*k Mod 26 =12*٤%26=48%26=22 (w).
- E (p) =P*k Mod 26 =15*٤%26=60%26=8 (i).
- E (u) =P*k Mod 26 =20*٤%26=80%26=2 (c).
- E (t) =P*k Mod 26 =19*٤%26=76%26=24 (y).

- E (e) =P*k Mod 26 =4*٤%26=16%26=16 (q).
- E (r) =P*k Mod 26 =17*٤%26=68%26=16 (q).

لەم حاڵەتەدا، ئەگەر سەرنج بدەین دەبینین ئەوا ژمارەیەك پیتی جیاواز لە نووسینەکەدا، گۆراوە بۆ هەمان پیت لە تەشفیرەکەدا، ئەمەش هەڵەیە و، ناگونجێت لە کرداری تەشفیر بەم ڕێگەیە.

نمونەی ٢:

بە بەکارهێنانی ئەلگۆریسمی Algorithm**ی لێکدان** Multiplicative**، نووسینی ئاسایی** Plain Text **ی وشەی زانکۆ** University **بگۆڕە بۆ وشەیەك کۆد بێت و نەخوێندرێتەوە** Encrypted.

تیبینی: لە خانەی سفرەوە Index = 0 **دەست پێ بکە.**

وەڵام:

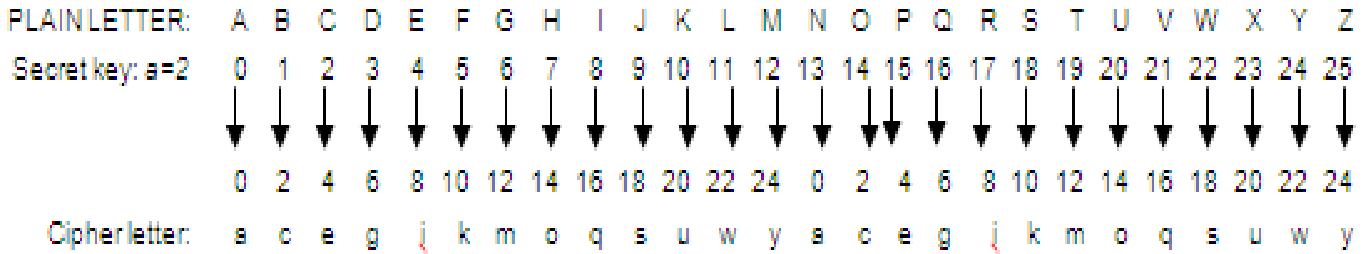
نمونەی ٣: بە بەکارهێنانی ئەلگۆریسمی Algorithmی لێکدان Multiplicative،ئەم نامە و پەیامە ئاساییەی خوارەوە بگۆرە بۆ هێما Cipher Text، کلیل =٧

Plain Text	t	h	e	s	k	y	i	s	b	l	u	e
Value												
x 7												
mod 26												
Cipher Text												

تیبینی: لە خانەی یەکەوە Index = 1 دەستپێبکە، بۆ ریزکردنی ئەلف بێ لە ریزکراوە Arrayدا.

نمونەی ٤:

ئەگەر کلیلەکە یەکسانبێت بە دوو Key = 2ئەوا هەنگاوەکانی ئەم ئەنجامانەی خوارەوە بنووسە:



وەڵام:

گۆڕینی کۆد بۆ نووسینی ئاسایی

Decryption in Multiplicative Cipher

ئەگەر نامە و پەیامێکی نوێمان دەست کەوتبێت لە ئەنجامی کرداری تەشفیرەوە Encrypted، وەك لە پێشتر باسمان کرد، بۆ نمونە ئەگەر بە کلیلی پێنج Key = 5 کردارەکەمان ئەنجام دابێت، ئەوا بە سوود وەرگتن لە کلیلی پێچەوانەی Inverse Key دەتوانین کردارەکە پێچەوانە بکەینەوە و، نامە و پەیامە نوێیەکە، کە ناروونە و لێی تێناگەین بکەینەوە بە نامە و پەیامە روون و ئاشکراکە Plain Text. لەم خشتەیەی خوارەوەدا، کلیلە پێچەوانەکان رووونکراوەتەوە Inverse Key،

ئەگەر نامە و پەیامێکی بە کۆد کراومان لەبەر دەست بوو و، زانیمان کە بەم رێگەیە کراوە بە کۆد Encoded، بە بەکارهێنانی کلیلی حەوت Key = 7، ئەوا بۆ دیکۆد Decode کردنی پێویستە، نرخی هەر یەکێك لە پیتەکان لە کلیلە پێچەوانەکە Inverse Key بدەین Multiply، کە پانزەیە ((۱۵)) هەروەها دۆزینەوەی مۆدی بیست و شەش Mod 26، بەڵام ئەمە سەلێنراوە نییە This may not be intuitive .

کلیلەکانی لێکدان و پێچەوانەکانیان

Multiplicative Keys and Inverses

Plaintext e is	Encode Key	Decode Key
O	3	9
Y	5	21
I	7	15
S	9	3
C	11	19
W	15	7
G	17	23
Q	19	11
A	21	5
K	23	17

U	25	25

نمونە:

ئەگەر کلیلی گۆرینی پەیامێك Encrypted Key بکاتە ١٧ بۆ گۆرینی پەیامێك بۆ ئەم ئەنجامە MGG BMG QBB FGH GQY F ، ئیستا ئەم ئەنجامە بگۆڕەوە بۆ نامە و پەیامێکی ڕوون و ئاسایی Plain Textبە بەکارهێنانی کلیلی پێچەوانە .

تیبینی: لە خانەی یەکەوە Index = 1 دەستپێبکە، بۆ ڕیزکردنی ئەلف بێ لە ڕیزکراوە Arrayدا.

وەڵام:

Multiplicative Decryption

Cipher Text	M	G	G	B	M	G	Q	B	B	F	G	H	G	Q	Y	F
value	13	7	7	2	13	7	17	2	2	6	7	8	7	17	25	6
x 23	299	161	161	46	299	161	391	46	46	138	161	184	161	391	575	138
mod 26	13	5	5	20	13	5	1	20	20	8	5	2	5	1	3	8
Plain Text	m	e	e	t	m	e	a	t	t	h	e	b	e	a	c	h

ئەنجام بریتییە لە :

Meet me at the beach

تیبینی:

ئەگەر لەم نمونەیەی سەرەوەدا، کلیلەکەنەدرایە و نەمان زانیایە، ئەوا پێتەکانمان دەژمارد و، دەبینین پێنج جی (5G) هەیە، هەروەها سێ بی (3B) و، جی زۆرترین دووبارە بوونەوەیە و، نرخی جی لە خشتەکە سەرەوەدا، دەکاتە حەڤدە ((١٧)) بۆ Encryption و، بۆ Decryption و پێچەوانە کردنەوەکەی کردبیە ٢٣، کە کلیلی پێچەوانە Inverse Key ی ١٧ یە.

بۆیە دەتوانین ئەم ڕێگەیەش بەکاربهێنین بۆ دیاری کردنی کلیل Key و، کلیلی پێچەوانە Inverse Key بۆ شیکار کردنی پرسیارەکان و، ئەنجامدانی Decryption و، گۆرینی نووسینە ناڕوون و تەشفیرەکان

Encrypted بۆ نووسینه روون و ئاشکراکان Plain Text.

نمونەی ٢:

ئەم نامە و پەیامە بە هێماکراوەی خوارەوە Cipher بگێڕەوە بۆ شێوە نووسینی ئاسایی Plain Text کە بخوێنرێتەوە و بزانرێت چییە، بە ئەلگۆریسی لێکدان:

Multiplicative Decryption: You intercept this message from the enemy and think it uses an multiplicative cipher.

Cipher Text	B	C	K	H	C	L	J	C	A	J	C	C	L	J	C	P	C
Value																	
x inverse																	
mod 26																	
Plain Text																	

تیبینی: لە خانەی یەکەوە Index = 1 دەستپێبکە، بۆ ریزکردنی ئەلف بێ لە ریزکراوە Arrayدا.

ئەنجام:

بەرنامەیەك بنووسە بۆ سایفەری لیکدان

Write Program to Multiplicative Cipher

```
//Hemn Barznji  _____ Multiplicative_Cipher
class Multiplicative_Cipher{
        int key[]={1,3,5,7,9,11,15,17,19,21,23,25};
        int i, z,l, ke=9, k,cS,cC,cNs,cNc;
        String ci="HemnBarznji 1982 / dr.hemn@yahoo.com";

char []ar={'A','B','C','D','E','F','G','H','I','J','K','L','M',
         'N','O','P','Q','R','S','T','U','V','W','X','Y','Z'};
char []arS={'a','b','c','d','e','f','g','h','i','j','k','l','m',
          'n','o','p','q','r','s','t','u','v','w','x','y','z'};
char []pla=ci.toCharArray();
void m(){
char []ar2=new char[pla.length];
for(int m=0; m<key.length; m++){
  if(ke%26==key[m]){
  k=ke;
for( z=0;z<pla.length;z++){
for(i=0;i<ar.length;i++){
if(pla[z]==ar[i]){
```

```
        cC=(i*k)%26;
          i=cC;
          ar2[z]=ar[i];
break;    }
 else{
          ar2[z]=pla[z]; }     }

for(l=0;l<arS.length;l++){
if(pla[z]==arS[l]){
        cS=(l*k)%26;
                l=cS;
                ar2[z]=arS[l];
      break;    }
 else{     }

}
}
}
}
String s= new String(ar2);
System.out.println(" "+s);
```

```
}
public static void main (String[] args){
Multiplicative_Cipher ob=new Multiplicative_Cipher ();
ob.m();
}
}
```

بەرنامەیەك بنووسە بۆ سیزەر و لیکدان

Write Program to Caesar and Muliplicative

```
//caser & multiplicative
class Mix_cipher{
String s;
                int key[]={1,3,5,7,9,11,15,17,19,21,23,25};
        int i, z,l, ke=9, k1,cS,cC,cNs,cNc;
   int  k=389756;
        String ci="HemnBarznji 1982 / dr.hemn@yahoo.com";
char []ar={'A','B','C','D','E','F','G','H','I','J','K','L','M',
         'N','O','P','Q','R','S','T','U','V','W','X','Y','Z'};
char []arS={'a','b','c','d','e','f','g','h','i','j','k','l','m',
         'n','o','p','q','r','s','t','u','v','w','x','y','z'};
```

```
char []pla=ci.toCharArray();
void m(){
char []ar2=new char[pla.length];
for( z=0;z<pla.length;z++){
for(i=0;i<ar.length;i++){
cC=(i+k)%26;
if(pla[z]==ar[i]){
        i=cC;
        ar2[z]=ar[i];
break;      }

else{
      ar2[z]=pla[z];   }    }
//////////////////
for(l=0;l<arS.length;l++){
      cS=(l+k)%26;
if(pla[z]==arS[l]){
              l=cS;
              ar2[z]=arS[l];
  break;
```

```
}
else{
}
}
}
}
s= new String(ar2);
System.out.println(" caser cipher is =   "+s);
}
void mm(){
char []pla=s.toCharArray();
char []ar2=new char[pla.length];
for(int m=0; m<key.length; m++){
  if(ke%26==key[m]){
  k1=ke;
for( z=0;z<pla.length;z++){
for(i=0;i<ar.length;i++){
if(pla[z]==ar[i]){
        cC=(i*k1)%26;
          i=cC;
          ar2[z]=ar[i];
break;   }
```

```
else{     ar2[z]=pla[z];    }
}
for(l=0;l<arS.length;l++){
if(pla[z]==arS[l]){
        cS=(l*k1)%26;
                l=cS;
                ar2[z]=arS[l];
      break;    }
 else{    }
}      }     }         }
String s= new String(ar2);
System.out.println(" multi cipher is =   "+s);      }
public static void main (String[] args){
Mix_cipher ob=new Mix_cipher();
ob.m();
ob.mm();
}
}
```

سایفەری ئەفاین

Affine Cipher

ئەم جۆرەی سایفەر هەردوو کرداری زیاد کردن Adding واتە Shiftingو، لێکدان Multiplicationلە خۆ دەگرێت و، بەهەردووکیان گۆرانکاری ئەفاین پێکدەهێنن، بە بەکارهێنانی ئەم یاسایەی خوارەوە :

$E_{k1, k2}(M) = (plain\ Text * Key\ 1 + Key\ 2) \bmod 26$

بەلام مەرجە کلیلی یەکەم Key 1 هەمان مەرجەکانی کلیلی سایفەری لێکدانی تێدابێت.

gcd(s, 26) must be 1

ئەم خشتەیەی پیتەکان بەکاردەهێنین بۆ دیاری کردنی شوینی پیتەکانی نامە و پەیامەکە:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

نمونە ی ١:

ئەگەر نووسینە روون و ئاشکراکەمان Plain Text بریتیبێت لە وشەی کۆلێژ College، بیگۆرە بۆ سایفەری ئەفاین، بەبەکارهێنانی حەوت وەك کلیلی یەکەم Key 1 = 7 و، ژمارە چوار وەکو کلیلی دووەم Key 2 =4.

وەڵام:

١. سەرەتا پیتەکانی زمانی ئینگلیزی لە خشتەیەك دا، دەنووسین:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

٢. یاسای سایفەری ئەفاین Affine Cipher کە بریتییە لەم یاسەیەی خوارەوە بەکاردەهێنین.

$E_{k1, k2}$ (M) = (plain Text * Key 1+Key 2) Mod 26

٣. یاساکە بەسەر هەریەکێك لە پیتەکانی وشەی collegeدا، جێبەجێدەکەین، بەم جۆرەی لای خوارەوە:

- $E_{k1, k2}$ (c) = (p* K1+K2) Mod26 = (2*7+4) %26=18%26=18 (s).
- $E_{k1, k2}$ (o) = (p* K1+K2) Mod26 = (14*7+4) %26= 102%26=24 (y).
- $E_{k1, k2}$ (l) = (p* K1+K2) Mod26 = (11*7+4) %26=81 %26=3 (d).
- $E_{k1, k2}$ (l) = (p* K1+K2) Mod26 = (11*7+4) %26=81 %26=3 (d).
- $E_{k1, k2}$ (e) = (p* K1+K2) Mod26 = (4*7+4) %26 =32 %26= 6 (g).
- $E_{k1, k2}$ (g) = (p* K1+K2) Mod26 = (6*7+4) % 26 = 46 %26 = 20 (u).
- $E_{k1, k2}$ (e) = (p* K1+K2) Mod26 = (4*7+4) %26 =32 %26= 6 (g).

٤. ئەنجامی کۆتایی بەم شێوەیەیە، و وشەی کۆلێژ College بووبە:

Cipher (c) = syddgug

نموونەی ٢:

بە بوونی ئەم زانیارییانەی لای خوارەوە و، بە سایفەری ئەفاین، بە کۆد کردن Encryption ئەنجامبدە:

تیبینی: لە خانەی یەکەوە Index = 1 دەستپێبکە، بۆ ریزکردنی ئەلف بێ لە ریزکراوە Arrayدا.

Plain Text = HERE BE DRAGONS.

Key 1 = 5.

Key 2 = 8.

تێبینی: ئەگەر وەلامەکەت ئەمەی لای خوارەوە نەبوو، کەواتە کارەکەت هەڵەیە:

ciphertext: rcpc nc xpimavu.

دی سایفەری ئەفاین

Deciphering (Decryption) Affine

ئەگەر نامە و پەیامێکی نوێمان دەست کەوتبێت لە ئەنجامی کرداری تەشفیرەوە Encrypted، وەك لە پێشتر باسمان کرد، بۆ نمونە ئەگەر بە کلیلی حەوت Key = 7 کردارەکەمان ئەنجام دابێت، ئەوا بە سوود وەرگتن لە کلیلی پێچەوانەی Inverse Key دەتوانین کردارەکە پێچەوانە بکەینەوە و، نامە و پەیامە نوێیەکە، کە ناروونە و لێی تێناگەین بکەینەوە بە نامە و پەیامە روون و ئاشکراکە Plain Text. لەم خشتەیەی خوارەوەدا، کلیلە پێچەوانەکان رووندکراوەتەوە Inverse Key،

ئەگەر نامە و پەیامێکی بە کۆد کراومان لەبەر دەست بوو و، زانیمان کە بەم رێگەیە کراوە بە کۆد Encoded، بە بەکارهێنانی کلیلی پێنج Key = 5، ئەوا بۆ دیکۆد Decode کردنی پێویستە، نرخی هەر یەکێك لە پیتەکان کلیلی دووەمی لێدەربکەین و پاشان لە کلیلە پێچەوانەکە Inverse Key بدەین Multiply، کە پانزەیە ((۲۱)) هەروەها دۆزینەوەی مۆدی بیست و شەش Mod 26، بەڵام ئەمە سەلێنراوە نییە This may not be intuitive .

کلیلەکانی ئەفاین و پێچەوانەکانیان

Affine Keys and Inverses

Plaintext e is	Encode Key	Decode Key
O	3	9
Y	5	21
I	7	15
S	9	3
C	11	19
W	15	7

G	17	23
Q	19	11
A	21	5
K	23	17
U	25	25

بە بەکارهێنانی ئەم یاسایە:

Plain Text = Key Invers * (Cipher – Key2) Mod 26

$P=K1^{-1}*(C-K2)\%26$

نمونە :

ئەگەر بمانەوێت ئەم رستەیەی لای خوارەوە بە سایفەری ئەفاین بگوێرین، بە بەکارهێنانی کلیلی 5 و، کلیلی ۷،

Defend the east wall of the castle

ئەواکاتێك پیتی دی D دەگوێرین بەم جۆرە دەردەچێت:

$E_{k1, k2}(d) = (p* K1+K2) Mod26 = (3*5+7) \%26=22\%26=22 (w)$

بەم شێوەیە هەمووی دەگوێرین هەتاوەکو دەبێتە سایفەر Encrypt، بەم شێوەی لای خوارەوە ئەنجامەکەمان دەست دەکەوێت:

wbgbuwyqbbhtynhkkzgyqbrhtykb

ئێستا بۆ دیکۆد Decode واتە Decryption کردنی، ئەنجامەکە و، گێرانەوەی بۆ نووسینە ئاساییەکە Plain Text، کلیلی پێچەوانە Key Invers بۆ کلیلی یەکەم وەردەگرین و، بەکاری دەهێنین، بە گوێرەی خشتەکەی سەرەوە ، کلیلی پێچەوانەیی پێنج (٥) دەکاتە ٢١، پاشان بەم یاسایە دی سایفەری دەکەینەوە:

$D (P) = K1^{-1}*(c-K2) Mod 26$

بۆ پیتی یەکەم:

D (w) =21*(c-7) Mod26

D (w) = 21 *(22 – 7) %26 = 21 * (15) %26= 315%26=3 (d).

هەمان کردار بۆ پیتەکانی تریش ئەنجام دەدەین.

بەرنامەیەك بنووسە بۆ سایفەری ئەفاین

Write Program to Affine Cipher

```
//Hemn Barznji  ------Affine_Cipher
class Affine_Cipher{
        int key[]={1,3,5,7,9,11,15,17,19,21,23,25};
         int k2=3, ke=9, k1,i,z,l,cS,cC,cNs,cNc;
        String ci="Hemn Barznji / dr.hemn@yahoo.com";
char []ar={'A','B','C','D','E','F','G','H','I','J','K','L','M',
         'N','O','P','Q','R','S','T','U','V','W','X','Y','Z'};
char []arS={'a','b','c','d','e','f','g','h','i','j','k','l','m',
          'n','o','p','q','r','s','t','u','v','w','x','y','z'};

char []pla=ci.toCharArray();
void m(){
char []ar2=new char[pla.length];
for(int m=0; m<key.length; m++){
  if(ke%26==key[m]){
  k1=ke;
```

```
for( z=0;z<pla.length;z++){
for(i=0;i<ar.length;i++){
if(pla[z]==ar[i]){
        cC=(i*k1+k2)%26;
         i=cC;
         ar2[z]=ar[i];
break;     }

 else{  ar2[z]=pla[z];   }
}
for(l=0;l<arS.length;l++){
if(pla[z]==arS[l]){
        cS=(l*k1+k2)%26;
                l=cS;
                ar2[z]=arS[l];
    break;
}
 else{       }
}
}
}
```

```
}
String s= new String(ar2);
System.out.println(" "+s);
}
public static void main (String[] args){
Affine_Cipher ob=new Affine_Cipher();
ob.m();
}
}
```

وشەکلیلی تێکەڵکراو

Keyword Mix

لەم ڕێگەیەدا، پێویستمان بە وشە کلیلێکی سەرەکی Keyword هەیە، بۆ نموونە وەکو Mathematics ، لەگەڵ کلیلێکی پیتی Key Letter، بۆ نموونە وەکو ئێس S.

پاشان ، جیبەجیکردن ی ئەم هەنگاوانەی لای خوارەوە :

١. پیتە دوو بارەکانی وشە کلیلەکە Keyword لادەبەین، بەمەش Matheics مان دەست دەکەوێت.

٢. یەکەم پیتی وشەکلیلە نوێ یەکەی دووبارەکانمان تیا لابردووە، لە ژێر کلیلە پیتەکەدا Key Letter دادەنێن و، پیتەکانی تریش بە دووای دا.

٣. پاشان ریزکراوەکە Array کە پیتەکانی تێدایە، تەواو دەکەین بە پیتەکانی تر، جگە لەو پیتانەی لەناو وشە کلیلە دەستکاری کراوەکەدا هەبوو، بێ دووبارە کردنەوەی پیت.

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
b	d	f	g	j	k	l	n	o	p	q	r	u	v	w	x	y	z	m	a	t	h	e	i	c	s

٤. ئیستا ئەو پلەین تێکستەی هەمان دەیگۆرین بە سایفەر تێکست، بۆ نموونە وشەی College، کە هەر پیتێکی وشەی College، لە ژێریدا پیتێك هەیە و، ئەو پیتە دەبێتە سایفەر، واتە بۆ Encryption لەسەرەوە بۆ خوارەوە وەری دەگرین و، بۆ Decryption بە پێچەوانەوە و لە خوارەوە بۆ سەرەوە:

Plain Text= College

Cipher Text=fwrrjlj

بەرنامەیەك بنووسە بۆ ئەنجامدانی کرداری بەهیماکردن و پیچەوانە کردنەوە بە جاڤا

Write Programe to Keyword Mix Encryption and Decryption

```
import java.awt.*;
import java.awt.event.*;
import javax.swing.*;
import javax.swing.GroupLayout;
import javax.swing.LayoutStyle;
import javax.swing.border.*;
/*
 * Created by JFormDesigner */
/**    * @author Hemn Barznji */
public class Keywordmixed extends JFrame {


          static char
[]array={'A','B','C','D','E','F','G','H','I','J','K','L','M','N','O','P','Q','R','S','T','U','V','W','X','Y','Z'};
        char []array2={'a','b','c','d','e','f','g','h','i','j','k','l','m','n','o','p','q','r','s','t','u','v','w','x','y','z'};


          static char
[]array1={'A','B','C','D','E','F','G','H','I','J','K','L','M','N','O','P','Q','R','S','T','U','V','W','X','Y','Z'};



   int number[]={1,3,5,7,9,11,15,17,19,21,23,25};
   static char []encryptArray=new char[26];
```

```
    static char [][]array3;
        static char []encryptArray1;
    static String print;
        public Keywordmixed() {
            initComponents();
            setVisible(true);
        }
        private void button7ActionPerformed(ActionEvent e) {
            // TODO add your code here
                //textArea7.setText("");
              key();
        }

        private void button8ActionPerformed(ActionEvent e) {
            // TODO add your code here
              String Cipher=textArea7.getText();
              textArea8.append(mixDecryption(Cipher));

        }

        private void initComponents() {
            // JFormDesigner - Component initialization - DO NOT MODIFY  //GEN-
BEGIN:initComponents
            panel7 = new JPanel();
            label10 = new JLabel();
            textField1 = new JTextField();
```

```
label11 = new JLabel();
comboBox1 = new JComboBox();
scrollPane7 = new JScrollPane();
panel10 = new JPanel();
scrollPane8 = new JScrollPane();
textArea7 = new JTextArea();
scrollPane9 = new JScrollPane();
panel11 = new JPanel();
scrollPane10 = new JScrollPane();
textArea8 = new JTextArea();
button7 = new JButton();
button8 = new JButton();

//======== this ========
setBackground(new Color(255, 153, 153));
setTitle("KeyWord Mixed");
Container contentPane = getContentPane();

//======== panel7 ========
{
        panel7.setBackground(Color.lightGray);
        panel7.setBorder(LineBorder.createBlackLineBorder());

        //---- label10 ----
        label10.setText("KeyWord");
        label10.setFont(label10.getFont().deriveFont(label10.getFont().getStyle() |
```

```
Font.BOLD, label10.getFont().getSize() + 1f));


                    //---- label11 ----

                    label11.setText("Letter");

                    label11.setFont(label11.getFont().deriveFont(label11.getFont().getStyle() |
Font.BOLD, label11.getFont().getSize() + 1f));


                    //---- comboBox1 ----


        comboBox1.setFont(comboBox1.getFont().deriveFont(comboBox1.getFont().getStyle() |
Font.BOLD));

                    comboBox1.setMaximumRowCount(9);

                    comboBox1.setModel(new DefaultComboBoxModel(new String[] {

                        "A ",

                        "B ",

                        "C",

                        "D",

                        "E",

                        "F",

                        "G",

                        "H",

                        "I",

                        "J",

                        "K",

                        "L",

                        "M",

                        "N",
```

```
                "O",
                "P",
                "Q",
                "R",
                "S",
                "T",
                "U",
                "V",
                "W",
                "X",
                "Y",
                "Z"
        }));
        comboBox1.setBackground(Color.pink);

        //======== scrollPane7 ========
        {

            //======== panel10 ========
            {
                panel10.setBorder(new
TitledBorder(UIManager.getBorder("CheckBox.border"), "Input File", TitledBorder.CENTER,
TitledBorder.TOP));
                panel10.setForeground(Color.red);
                panel10.setBackground(new Color(204, 204, 204));
                panel10.setLayout(new BorderLayout(2, 2));
```

```
                    //======== scrollPane8 ========
                    {
                        scrollPane8.setViewportView(textArea7);
                    }
                    panel10.add(scrollPane8, BorderLayout.CENTER);
                }
                scrollPane7.setViewportView(panel10);
            }

            //======== scrollPane9 ========
            {

                //======== panel11 ========
                {
                    panel11.setBorder(new
TitledBorder(UIManager.getBorder("CheckBox.border"), "Output File", TitledBorder.CENTER,
TitledBorder.TOP));
                    panel11.setBackground(new Color(204, 204, 204));
                    panel11.setLayout(new BorderLayout(2, 2));

                    //======== scrollPane10 ========
                    {
                        scrollPane10.setViewportView(textArea8);
                    }
                    panel11.add(scrollPane10, BorderLayout.CENTER);
                }
                scrollPane9.setViewportView(panel11);
```

```
}

//---- button7 ----
button7.setText("Encrypt File");
button7.setFont(new Font("Tahoma", Font.BOLD, 14));
//button7.setBackground(Color.black);
button7.addActionListener(new ActionListener() {
        @Override
        public void actionPerformed(ActionEvent e) {
                button7ActionPerformed(e);
        }
});

//---- button8 ----
button8.setText("Decrypt File");
button8.setFont(new Font("Tahoma", Font.BOLD, 14));
//button8.setBackground(Color.black);
button8.addActionListener(new ActionListener() {
        @Override
        public void actionPerformed(ActionEvent e) {
                button8ActionPerformed(e);
        }
});

GroupLayout panel7Layout = new GroupLayout(panel7);
panel7.setLayout(panel7Layout);
```

```
                panel7Layout.setHorizontalGroup(
                        panel7Layout.createParallelGroup()
                                .addGroup(panel7Layout.createSequentialGroup()
                                        .addContainerGap()
                                        .addGroup(panel7Layout.createParallelGroup()
        .addGroup(panel7Layout.createParallelGroup(GroupLayout.Alignment.LEADING, false)
                                                        .addComponent(scrollPane7,
GroupLayout.DEFAULT_SIZE, 282, Short.MAX_VALUE)
        .addGroup(panel7Layout.createSequentialGroup()
        .addGroup(panel7Layout.createParallelGroup()
                                                                .addComponent(label10,
GroupLayout.PREFERRED_SIZE, 84, GroupLayout.PREFERRED_SIZE)
                                                                .addComponent(label11,
GroupLayout.PREFERRED_SIZE, 61, GroupLayout.PREFERRED_SIZE))
        .addPreferredGap(LayoutStyle.ComponentPlacement.RELATED)
        .addGroup(panel7Layout.createParallelGroup(GroupLayout.Alignment.LEADING, false)
        .addComponent(comboBox1, 0, GroupLayout.DEFAULT_SIZE, Short.MAX_VALUE)
        .addComponent(textField1, GroupLayout.DEFAULT_SIZE, 194, Short.MAX_VALUE)))
                                                        .addComponent(scrollPane9))
        .addGroup(panel7Layout.createSequentialGroup()
                                                        .addComponent(button7,
GroupLayout.DEFAULT_SIZE, GroupLayout.DEFAULT_SIZE, Short.MAX_VALUE)
```

```
                                        .addGap(39, 39, 39)
                                        .addComponent(button8)
                                        .addGap(475, 475, 475))))
                );
                panel7Layout.setVerticalGroup(
                        panel7Layout.createParallelGroup()
                                .addGroup(panel7Layout.createSequentialGroup()
                                        .addContainerGap()

        .addGroup(panel7Layout.createParallelGroup(GroupLayout.Alignment.BASELINE)
                                                .addComponent(label10,
GroupLayout.PREFERRED_SIZE, 28, GroupLayout.PREFERRED_SIZE)
                                                .addComponent(textField1,
GroupLayout.PREFERRED_SIZE, GroupLayout.DEFAULT_SIZE, GroupLayout.PREFERRED_SIZE))

        .addPreferredGap(LayoutStyle.ComponentPlacement.RELATED)

        .addGroup(panel7Layout.createParallelGroup(GroupLayout.Alignment.BASELINE)
                                                .addComponent(label11,
GroupLayout.PREFERRED_SIZE, 24, GroupLayout.PREFERRED_SIZE)
                                                .addComponent(comboBox1,
GroupLayout.PREFERRED_SIZE, 21, GroupLayout.PREFERRED_SIZE))
                                        .addGap(18, 18, 18)
                                        .addComponent(scrollPane7,
GroupLayout.PREFERRED_SIZE, 80, GroupLayout.PREFERRED_SIZE)

        .addPreferredGap(LayoutStyle.ComponentPlacement.UNRELATED)
                                        .addComponent(scrollPane9,
GroupLayout.PREFERRED_SIZE, 72, GroupLayout.PREFERRED_SIZE)
                                        .addGap(18, 18, 18)
```

```
                                        .addGroup(panel7Layout.createParallelGroup()
                                                .addComponent(button7)
                                                .addComponent(button8))
                                        .addContainerGap(24, Short.MAX_VALUE))
                        );
                }

                GroupLayout contentPaneLayout = new GroupLayout(contentPane);
                contentPane.setLayout(contentPaneLayout);
                contentPaneLayout.setHorizontalGroup(
                        contentPaneLayout.createParallelGroup()
                                .addGroup(contentPaneLayout.createSequentialGroup()
                                        .addContainerGap()
                                        .addComponent(panel7, GroupLayout.PREFERRED_SIZE, 318,
GroupLayout.PREFERRED_SIZE)
                                        .addContainerGap(GroupLayout.DEFAULT_SIZE,
Short.MAX_VALUE))
                );
                contentPaneLayout.setVerticalGroup(
                        contentPaneLayout.createParallelGroup()
                                .addGroup(contentPaneLayout.createSequentialGroup()
                                        .addContainerGap()
                                        .addComponent(panel7, GroupLayout.PREFERRED_SIZE,
GroupLayout.DEFAULT_SIZE, GroupLayout.PREFERRED_SIZE)
                                        .addContainerGap(GroupLayout.DEFAULT_SIZE,
Short.MAX_VALUE))
                );
```

```
                pack();
                setLocationRelativeTo(getOwner());
                // JFormDesigner - End of component initialization  //GEN-END:initComponents
        }

//----------------------------------KeywordMix-------------------------------------------



public static String keyWord(String word)
{
String s=word.toUpperCase();
char [] norepeat=s.toCharArray();
for(int i=0; i<norepeat.length;i++)
{
for(int j=i+1; j<norepeat.length;j++)
{
if(norepeat[i]==norepeat[j])
norepeat[j]=' ';
}
}
String ss="";
int k=0;
int l=0;
while(k<norepeat.length)
{
```

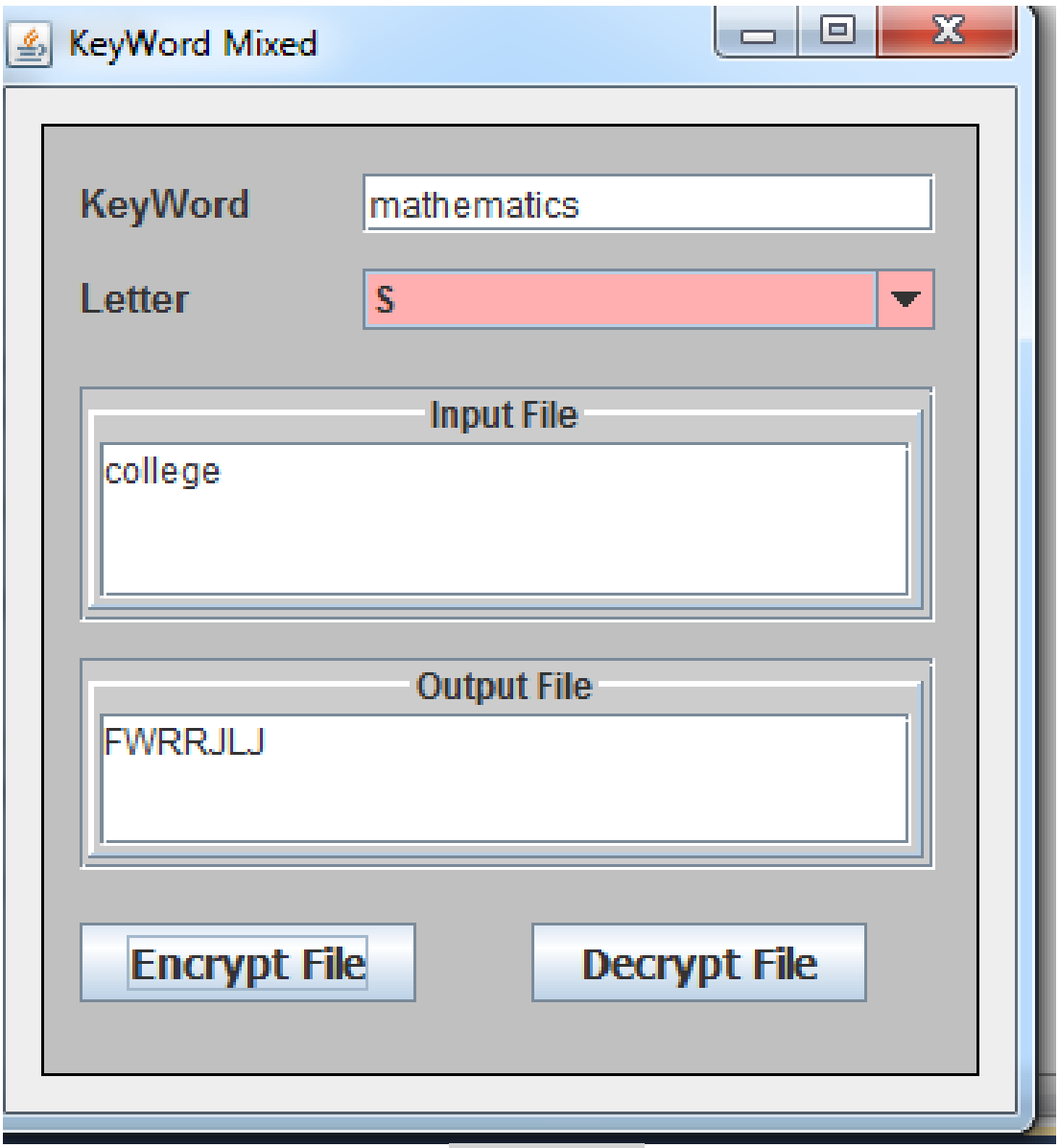
```
if(norepeat[k]!=' ')
ss+=norepeat[k];
k++;
}
norepeat=ss.toCharArray();
return new String (norepeat);

}
public static int keyLetter(String keyletter)
{
char ar=keyletter.charAt(0);
char c=Character.toUpperCase(ar);
for(int i=0;i<array.length;i++)
{
if(array[i]==c)
{
return i;
}
}
return 0;
}

public static String newArray(String keyWord,String keyletter)
{
 //char b=keyletter.charAt(0);
```

```
int index=keyLetter(keyletter);
int indexC=index;
char []word=keyWord(keyWord).toCharArray();
String ss="";
for(int i=0; i<word.length;i++)
{
encryptArray[index%26]=word[i];
index++;
}
for(int i=0; i<word.length;i++)
{
for(int j=0; j<array.length;j++)
{
if(array[j]==word[i])
array[j]=' ';
}
}
int x=index;
int y=0;
while(x%26!=indexC && y<array.length)
{
if(array[y]!=' ')
{
encryptArray[x%26]=array[y];
x++;
}
```

```
y++;
}
System.out.println(new String(encryptArray));
return new String(encryptArray);
}

public static String mixEncryption(String keyword,String keyletter,String plaintext)
{
newArray(keyword, keyletter);
String p=plaintext.toUpperCase();
char []plain=p.toCharArray();
for(int i=0;i<plain.length;i++)
{
for(int j=0;j<array1.length;j++)
{
if(plain[i]==array1[j])
{
plain[i]=encryptArray[j];
break;
}
}
}

return new String(plain);
}
public static String mixDecryption(String ciphertext)
```

```
{
String c=ciphertext.toUpperCase();
char []cipher=c.toCharArray();
for(int i=0;i<cipher.length;i++)
{
for(int j=0;j<array1.length;j++)
{
if(cipher[i]==encryptArray[j])
{
cipher[i]=array1[j];
break;
}
}
}
return new String(cipher);

}

        // JFormDesigner - Variables declaration - DO NOT MODIFY  //GEN-BEGIN:variables
        private JPanel panel7;
        private JLabel label10;
        private JTextField textField1;
        private JLabel label11;
        private JComboBox comboBox1;
        private JScrollPane scrollPane7;
        private JPanel panel10;
```

```
        private JScrollPane scrollPane8;
        private JTextArea textArea7;
        private JScrollPane scrollPane9;
        private JPanel panel11;
        private JScrollPane scrollPane10;
        private JTextArea textArea8;
        private JButton button7;
        private JButton button8;

        public void key(){
     String plain=textArea7.getText();
                String b=textField1.getText();
                Object o=comboBox1.getSelectedItem();
                String c=o.toString();
//              label12.setText(keyWord(b));
    // textArea8.append();
     textArea8.append(mixEncryption(b,c,plain));
                }

        // JFormDesigner - End of variables declaration  //GEN-END:variables
                public static void main(String[]args)
                {
                        new Keywordmixed();
        }
}
```



روونکردنەوە:

لەبەر ئەوەی درێژیی دیڕ لە بەرنامەی مایکرۆسۆفت ۆرد دیاری کراوە، بۆیە زۆر جار دیرە کۆد دەبیتە دوو دیر یان زیاتر لە بەرنامەی ۆرد ،دا بۆیە پێویستە لەکاتی نووسینەوەی بەرنامەکەدا ئاگاداری ئەو حالەتانەبن تا هەلەتان نەبێت و بەرنامەکە کار بکات.

وشە کلیلی تێکەڵکراوی گواستراوە

Transposed Keyword Mixed

وشەکلیلی تێکەڵکراویی گواستراوە Transposed Keyword Mixed یەکێکی تر لەو ئەلگۆریسمانەی کە بە بەکارهێنانی وشەکلیلی سەرەکی Keyword و دروستکردنی ریزکراوە کارەکە بە ئەنجام دەگات.

ئەم هەنگاوانەی خوارەوە پێویستن بۆ جیبەجێکردنی کرداریی سایفەر بە ئەم ئەلگۆریسمە.

یەکەم// دروستکردنی ریزکراوە بە بەکارهێنانی وشە کلیلی سەرەکی :

١. لەم رێگەیەدا پێویستە وشەکلیلیکی سەرەکیمان هەبێت Keyword بۆ نموونە MATHEMATHICS.
٢. دووای ئەوە پیتە دووبارەکانی ناو وشەکلیلەکە لادەبەین Remove Repeated Letter.
٣. ریزکراوەیەك Matrixدروست دەکەین کە ژمارەی ستوونەکانی Column دەکاتە ژمارەی پیتەکانی وشەکلیلەکە Keyword دووای لابردنی پیتە دووبارەکان.
٤. پاشان خانەکانی تری ریزکراوەکە Matrix پردەکەینەوە، بە پیتەکانی تری زمانی ئینگلیزی تا هەموو پیتەکان لە ریزکراوەکەدا هەبن بێ دووبارە بوونەوە ئەو پیتانەی لە وشە کلیلەکەدان Keyword.

M	A	T	H	E	I	C	S
B	D	F	G	J	K	L	N
O	P	Q	R	U	V	W	X
Y	Z						

ئەمەش یەکەم هەنگاوی کارەکەمان بوو کە ئامادەکردنی ریزکراوەیەك بوو، بەهۆی ئەو وشە کلیلە سەرەکییەی کە دراوە پێمان و بەهۆیەوە وشەی نووسینی ئاسایی دەگۆرین بۆ نووسینی نهێنی. ئیستاش هەنگاوی دووەم

جیبەجێدەکەین.

دووەم// بەکارهێنانی ریزکراوە Matrixی درووستکراو بۆ کردارەکان:

١. نووسینی ئاسایی Plain Text ئەلفبێی لە ریزێکدا Row دەنووسین.
٢. نووسینی سایفەر Cipher Txt ی ئەلفبێی لە ریزی دووەمدا دەنووسین، ئەویش بەنووسینی ستوونی یەکەم First Column ریزکراوەکە لە سەرەتای ئەم ریزەدا و، پاشان ستوونی دووەم و بەو شێوەیە تا دووا ستوون.

Plain Text Alphabet																									
A	B	C	D	E	F	G	H	I	J	K	L	M	N	o	P	Q	R	S	T	u	V	W	X	Y	Z
Cipher Text Alphabet																									
M	B	o	Y	A	D	P	Z	T	F	Q	H	G	R	E	J	U	I	K	V	C	L	W	S	N	X

سێهەم// ئیستا کرداری گۆرینی نووسینی ئاسایی Plain Textبۆ نووسینی هیمایی Cipher Text ئەنجام دەدەین:

١. نووسینە ئاساییە Plain Text دەنووسین.

بۆنموونە // وشەی نووسینی ئاسایی زانکۆ :

Plain Text:

University

٢. هەر پیتێك لە پیتەکانی نووسینە ئاساییەکە دەدۆزینەوە لە ریزی نووسینی ئاسایی ئەلفبێی Plain Text Alphabet ی سەرەوە و، لە ژێریدا واتە لە ریزی نووسینی هیمایی ئەلفبێی Cipher Text Alphabet، پیتەکەی دیاری دەکەین و دەینووسین، بۆ نموونە پیتی U لە ژێریدا پیتی C، هەیە و، پیتی N، لە ژێریدا پیتی R نووسراوە، پیتی ئای I لە ژێریدا T نووسراوە و بەو جۆرە بەردەوام بە تا کۆتا پیتی نووسینە ئاساییەکە و نووسینی هیماییەکەی :

Plain text : U N I V E R S I T Y

Cipher text: C R T L A I K T V N

تیبینی : واتە بۆ کرداری گۆرینی نووسینی ئاسایی Plain Text بۆ نووسینی سایفەر Cipher Text لەسەرەوە بۆ خوارەوە ئەژمارەکەین و وەری دەگرین.

Plain Text Alphabet																									
A	B	C	D	E	F	G	H	I	J	K	L	M	N	o	P	Q	R	S	T	u	V	W	X	Y	Z
Cipher Text Alphabet																									
M	B	o	Y	A	D	P	Z	T	F	Q	H	G	R	E	J	U	I	K	V	C	L	W	S	N	X

چووارەم// گۆڕینی نووسینی سایفەر Cipher Text بۆ نووسینی ئاسایی Plain Text.

دووای تەنجامدانی خاڵی ((یەکەم و... دووەم)) تەم هەنگاوانە جیبەجیدەکەین.

١. نووسینە سایفەرەکە Cipher Text دەنووسین، بۆ نمونە :

٢. پیت بە پیتی سایفەرەکە وەرەگرین و، لە ریزیی نووسینی سافەر Cipher Text دەیدۆزینەوە و بەرامبەرەکەی وەرەگرین لە ریزیی Plain Textدا. بۆنمونە پیتی سی C، بەرامبەرەکەی لە نووسینی ئاسایی دا U، پیتی R لە نووسینی سایفەر دا، بەرامبەرەکەی N لە نووسینی ئاسایی دا، بەهەمان شێوە هەموو پیتەکانی تریش دەدۆزینەوە و بەرامبەرەکەی وەرەگرین.

تیبینی : واتە بۆ کرداری گۆڕینی نووسینی سایفەر Cipher Text بۆ نووسینی ئاسایی Plain Text لە خوارەوە بۆ سەرەوە ئەژمارەکەین و وەری دەگرین.

Cipher text: C R T L A I K T V N

Plain text : U N I V E R S I T Y

Plain Text Alphabet																									
A	B	C	D	E	F	G	H	I	J	K	L	M	N	o	P	Q	R	S	T	u	V	W	X	Y	Z
Cipher Text Alphabet																									
M	B	o	Y	A	D	P	Z	T	F	Q	H	G	R	E	J	U	I	K	V	C	L	W	S	N	X

بەزمانی جاڤا بەرنامەیەك بنووسە بۆ گۆڕینی نووسینی ئاسایی بۆ هێما

Write Program to Convert Plain Text – Cipher Text Using Java

```
import java.awt.*;

import java.awt.event.*;

import javax.swing.*;
```

```
import javax.swing.GroupLayout;
import javax.swing.LayoutStyle;
import javax.swing.border.*;
/*
 * Created by JFormDesigner
 */

/**     * @author Hemn Barznji     */
public class Transposition extends JFrame {
        static char
[]array={'A','B','C','D','E','F','G','H','I','J','K','L','M','N','O','P','Q','R','S','T','U','V','W','X','Y','Z'};
       char []array2={'a','b','c','d','e','f','g','h','i','j','k','l','m','n','o','p','q','r','s','t','u','v','w','x','y','z'};
        static char
[]array1={'A','B','C','D','E','F','G','H','I','J','K','L','M','N','O','P','Q','R','S','T','U','V','W','X','Y','Z'};
   int number[]={1,3,5,7,9,11,15,17,19,21,23,25};
   static char []encryptArray=new char[26];
   static char [][]array3;
        static char []encryptArray1;
   static String print;

        public Transposition() {
                initComponents();
                setVisible(true);
        }

        private void button9ActionPerformed(ActionEvent e) {
```

```
            // TODO add your code here
            Transposition();
        }

    private void button10ActionPerformed(ActionEvent e) {
            // TODO add your code here
            setVisible(false);
        }

    private void initComponents() {
            // JFormDesigner - Component initialization - DO NOT MODIFY  //GEN-
BEGIN:initComponents
            panel12 = new JPanel();
            scrollPane12 = new JScrollPane();
            textArea10 = new JTextArea();
            scrollPane13 = new JScrollPane();
            textArea11 = new JTextArea();
            label14 = new JLabel();
            button9 = new JButton();
            button10 = new JButton();
            textField2 = new JTextField();

            //======== this ========
            setTitle("Transposition");
            Container contentPane = getContentPane();
```

```
            //======== panel12 ========
            {
                panel12.setBorder(LineBorder.createBlackLineBorder());
                panel12.setBackground(Color.lightGray);

                //======== scrollPane12 ========
                {
                    scrollPane12.setBorder(new
TitledBorder(UIManager.getBorder("CheckBox.border"), "Input File ", TitledBorder.CENTER,
TitledBorder.TOP));
                    scrollPane12.setViewportView(textArea10);
                }

                //======== scrollPane13 ========
                {
                    scrollPane13.setBorder(new
TitledBorder(UIManager.getBorder("CheckBox.border"), "Output File", TitledBorder.CENTER,
TitledBorder.TOP));

                    //---- textArea11 ----
                    textArea11.setBorder(null);
                    scrollPane13.setViewportView(textArea11);
                }

                //---- label14 ----
                label14.setText("keyWord");
                label14.setFont(label14.getFont().deriveFont(Font.BOLD,
```

```
label14.getFont().getSize() + 2f));

                //---- button9 ----
                button9.setText("Encryption");
                button9.setFont(new Font("Tahoma", Font.BOLD, 12));
                //button9.setBackground(Color.black);
                button9.addActionListener(new ActionListener() {
                        @Override
                        public void actionPerformed(ActionEvent e) {
                                button9ActionPerformed(e);
                        }
                });

                //---- button10 ----
                button10.setText("Exit");
                button10.setFont(new Font("Tahoma", Font.BOLD, 12));
                //button10.setBackground(Color.black);
                button10.addActionListener(new ActionListener() {
                        @Override
                        public void actionPerformed(ActionEvent e) {
                                button10ActionPerformed(e);
                        }
                });

                GroupLayout panel12Layout = new GroupLayout(panel12);
                panel12.setLayout(panel12Layout);
```

```
                panel12Layout.setHorizontalGroup(
                        panel12Layout.createParallelGroup()
                                .addGroup(panel12Layout.createSequentialGroup()
                                        .addContainerGap()
                                        .addGroup(panel12Layout.createParallelGroup()

        .addGroup(panel12Layout.createParallelGroup(GroupLayout.Alignment.LEADING, false)

        .addGroup(panel12Layout.createSequentialGroup()
                                                        .addComponent(label14,
GroupLayout.PREFERRED_SIZE, 69, GroupLayout.PREFERRED_SIZE)

        .addPreferredGap(LayoutStyle.ComponentPlacement.RELATED)
                                                        .addComponent(textField2,
GroupLayout.PREFERRED_SIZE, 108, GroupLayout.PREFERRED_SIZE))
                                                .addComponent(scrollPane12,
GroupLayout.DEFAULT_SIZE, 273, Short.MAX_VALUE)
                                                .addComponent(scrollPane13))

        .addGroup(panel12Layout.createSequentialGroup()
                                                .addGap(15, 15, 15)
                                                .addComponent(button9)
                                                .addGap(29, 29, 29)
                                                .addComponent(button10)))
                                        .addContainerGap(21, Short.MAX_VALUE))
                );
                panel12Layout.setVerticalGroup(
                        panel12Layout.createParallelGroup()
                                .addGroup(GroupLayout.Alignment.TRAILING,
```

```
panel12Layout.createSequentialGroup()
                                        .addContainerGap()

            .addGroup(panel12Layout.createParallelGroup(GroupLayout.Alignment.BASELINE)
                                                .addComponent(label14)
                                                .addComponent(textField2,
GroupLayout.PREFERRED_SIZE, GroupLayout.DEFAULT_SIZE, GroupLayout.PREFERRED_SIZE))
                                        .addGap(13, 13, 13)
                                        .addComponent(scrollPane12,
GroupLayout.PREFERRED_SIZE, 76, GroupLayout.PREFERRED_SIZE)
                                        .addGap(17, 17, 17)
                                        .addComponent(scrollPane13,
GroupLayout.PREFERRED_SIZE, 76, GroupLayout.PREFERRED_SIZE)
                                        .addGap(18, 18, 18)

            .addGroup(panel12Layout.createParallelGroup(GroupLayout.Alignment.BASELINE)
                                                .addComponent(button10,
GroupLayout.PREFERRED_SIZE, 44, GroupLayout.PREFERRED_SIZE)
                                                .addComponent(button9,
GroupLayout.PREFERRED_SIZE, 44, GroupLayout.PREFERRED_SIZE))
                                        .addGap(85, 85, 85))
                    );
                }

        GroupLayout contentPaneLayout = new GroupLayout(contentPane);
        contentPane.setLayout(contentPaneLayout);
        contentPaneLayout.setHorizontalGroup(
                contentPaneLayout.createParallelGroup()
```

```
                        .addGroup(contentPaneLayout.createParallelGroup()
                            .addGroup(contentPaneLayout.createSequentialGroup()
                                .addContainerGap()
                                .addComponent(panel12,
GroupLayout.PREFERRED_SIZE, GroupLayout.DEFAULT_SIZE, GroupLayout.PREFERRED_SIZE)
                                .addContainerGap(GroupLayout.DEFAULT_SIZE,
Short.MAX_VALUE)))
                        .addGap(0, 329, Short.MAX_VALUE)
                );
                contentPaneLayout.setVerticalGroup(
                    contentPaneLayout.createParallelGroup()
                        .addGroup(contentPaneLayout.createParallelGroup()
                            .addGroup(contentPaneLayout.createSequentialGroup()
                                .addContainerGap()
                                .addComponent(panel12,
GroupLayout.DEFAULT_SIZE, 287, Short.MAX_VALUE)
                                .addContainerGap()))
                        .addGap(0, 309, Short.MAX_VALUE)
                );
                pack();
                setLocationRelativeTo(getOwner());
                // JFormDesigner - End of component initialization  //GEN-END:initComponents
        }

//////////////////////////////Transposition

public static String keyWord(String word)
```

```
{
String s=word.toUpperCase();
char [] norepeat=s.toCharArray();
for(int i=0; i<norepeat.length;i++)
{
for(int j=i+1; j<norepeat.length;j++)
{
if(norepeat[i]==norepeat[j])
norepeat[j]=' ';
}
}
String ss="";
int k=0;
int l=0;
while(k<norepeat.length)
{
if(norepeat[k]!=' ')
ss+=norepeat[k];
k++;
}
norepeat=ss.toCharArray();
return new String (norepeat);

}

public static char[] newAlpha(char[]word)
```

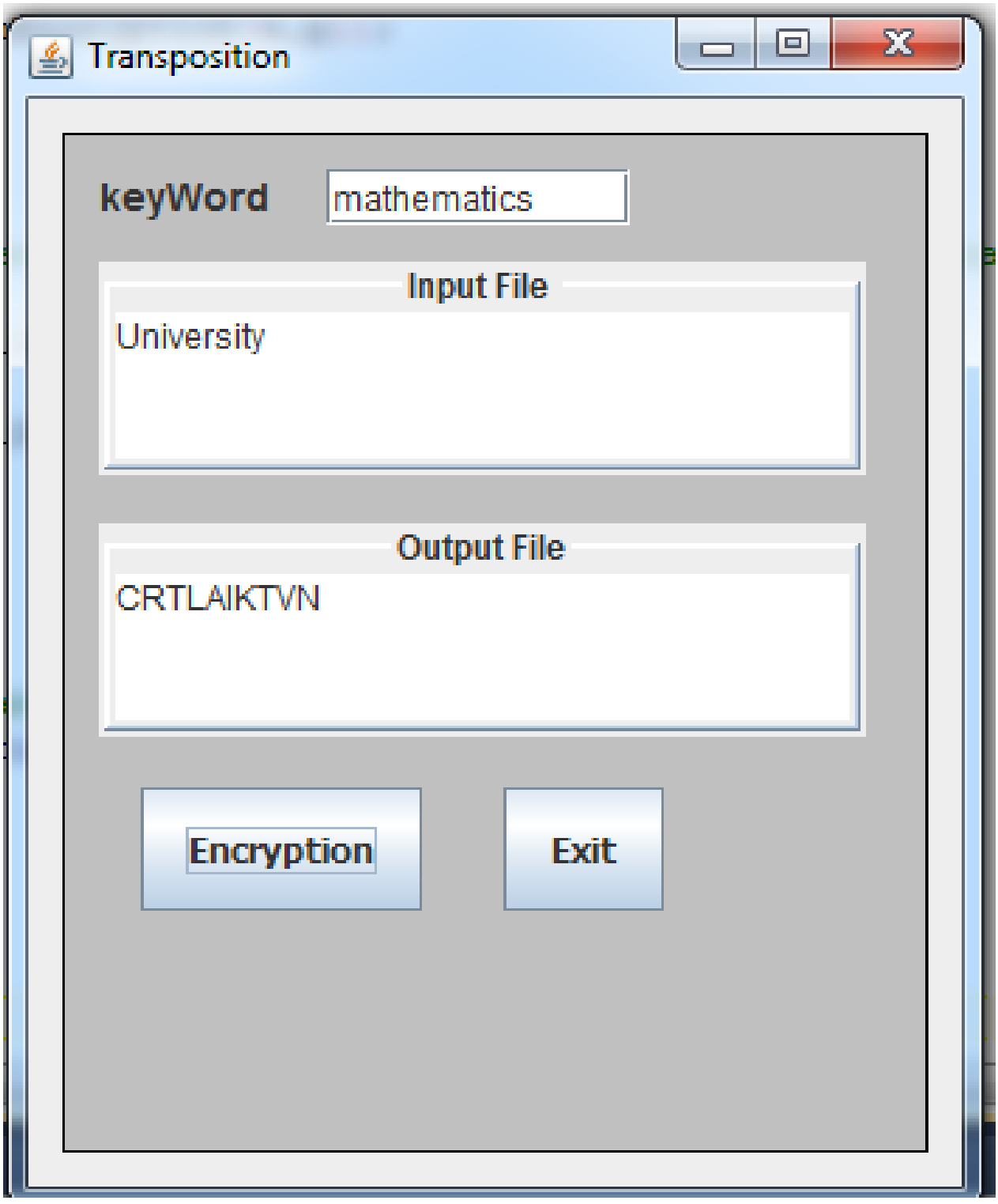
```
{
        for(int i=0; i<word.length;i++)
        {
         for(int j=0; j<array.length;j++)
         {
                if(array[j]==word[i])
                        array[j]=' ';
         }
        }
        String s3=new String(array);
         s3=s3.replace(" ","");
        System.out.println(s3);
        char []removeRepeatAlpha=s3.toCharArray();
        return removeRepeatAlpha;
}

        public static String newArray(String keyWord)
        {
                char []word=keyWord(keyWord).toCharArray();
                char []alph=newAlpha(word);
                double x= Math.ceil(26.0d/word.length);
                int row =(int)x;
                System.out.println(row);
                System.out.println(word.length);
                array3=new char[row][word.length];
                ////////////////////////////////////////first row
```

```
                int k=0;
                for(int i=0; i<word.length;i++)
                {
                        array3[k][i]=word[i];
                }
                ////////////////////////////////////second row ---->end
                k=-1;
                for(int i=1; i<row;i++)
                {
                        for(int j=0;j<word.length;j++)
                        {
                         k++;
                         if(k<alph.length)
                                array3[i][j]=alph[k];
                         else
                                array3[i][j]='&';

                        }
                }
            ////////////////////////////////////
        for(int i=0; i<row;i++)
                {
                for(int j=0; j<word.length;j++)
                {
                 // System.out.print(array[i][j]);

```

```
String  output=""+array3[i][j];
                // System.out.print(output);
                 // System.out.print(a);
                }
                 System.out.println();
                }
                ////////////////////////////////////
                encryptArray=new char[row*word.length];
                k=-1;
                for(int i=0; i<word.length;i++)
                {
                        for(int j=0;j<row;j++)
                        {
                        if(array3[j][i]=='&')
                                  break;
                                k++;
                                encryptArray[k]=array3[j][i];

                        }
                }
                String ss=new String (encryptArray);
          //      System.out.println(ss);
               ////////////////////////////
                return ss;
        }
        static char []alpha1
```

```
={'A','B','C','D','E','F','G','H','I','J','K','L','M','N','O','P','Q','R','S','T','U','V','W','X','Y','Z'};

public static String TranspositionEncryption(String keyword,String plaintext)
        {

                newArray(keyword);
                String p=plaintext.toUpperCase();
                char []plain=p.toCharArray();
                for(int i=0;i<plain.length;i++)
                {
                  for(int j=0;j<alpha1.length;j++)
                 {
                        if(plain[i]==alpha1[j])
                        {
                                plain[i]=encryptArray[j];
                                break;
                        }
                 }
                }
                String s=new String(plain);
                return s;
        }
  public void  Transposition(){
        String a=textField2.getText();
      String p=textArea10.getText();
//      label15.setText(newArray(a));
//      label16.setText(keyWord(a));

```

```
textArea11.append (TranspositionEncryption(a,p));
        }
        // JFormDesigner - Variables declaration - DO NOT MODIFY  //GEN-BEGIN:variables
        private JPanel panel12;
        private JScrollPane scrollPane12;
        private JTextArea textArea10;
        private JScrollPane scrollPane13;
        private JTextArea textArea11;
        private JLabel label14;
        private JButton button9;
        private JButton button10;
        private JTextField textField2;
        // JFormDesigner - End of variables declaration  //GEN-END:variables
                public static void main(String[]args)
                {
                        new Transposition();
        }
}
```


Transposition
keyWord
mathematics
Input File
University
Output File
CRTLAIKTVN
Encryption
Exit

بیلّ سایفەر

Beale Cipher

یەکێك لەو رێگە و ئەلگۆریسمانەی دیکەیە، کە بەکاردەهێنرێت بۆ تەشفیر کردن Encode (Encryption) ی نووسینێکی ئاسایی و ئاشکراو و رووn Plain Text، هەروەها بۆ لابردنەوەی تەشفیرەکە Decode (Decryption)، بە جێبەجێکردنی ئەم هەنگاوانەی لای خوارەوە:

١. لەم رێگە و ئەلگۆریسمەدا، ژمارە دەخریتە شوێنی پیتەکان، بۆ تەشفیر کردن، بە بەکار هێنانی سایفەری بووك Book Cipher کە ژمارە دادەنێین بۆ هەر یەکێك لە وشەکانی سایفەری بووك Book Cipher.

٢. نوسینە ئاسایی و رووندکە Plain Text تەشفیر دەکەین، بە لابردنی پیتەکان و دانانی ژمارە بۆ هەر یەکێك لە پیتەکانی، کە شوێنی پیتەکە پیشان دەدات لە نووسینی سایفەری بووك Book Cipher ، کە وشەکەی سایفەری بووك بەم پیتەی نوسینە ئاشکراو و رووندکە دەستپێدەکات.

نموونە:

ئەگەر سایفەری بووك Book Cipher بکات ئەم رستەیەی لای خوارەوە، ئەوا نووسینی ئاشکراو و رووندی نهێنی (Plain Text = secret) بگۆرە بۆ نووسینێکی تەشفیر کراو Encryption (Encode):

Cipher Book = seven crazy termites eat rotten elderberries

وەڵام:

١. ژمارە بۆ وشەکانی Book Cipher دادەنێین:

Seven	Crazy	Termites	Eat	Rotten	Elderberries
1	2	3	4	5	6

٢. نوسینه ئاشکراکه بریتییه له secret .

٣. بۆ گۆرین و تەشفیر کردنی secret سەیری وشەکانی Book Cipher دەکەین و، هەر وشەیەکی بووك سایفەر یەکەم پیتی بریتیبێت لە یەکێك لە پیتەکانی Plain Text ، ئەوا ئەو پیتەی Plain Text لا دەبەین و، لە ژێریا ژمارەی ئەو وشەیەی Cipher Book دەنووسین.

بووك سایفەر – Book Cipherپێکهاتووە لە :

Seven	Crazy	Termites	Eat	Rotten	Elderberries
1	2	3	4	5	6

وشەی ئاسایی Plain Text بریتییە لە secret و پێکهاتووە لە پیتەکانی :

s	e	c	r	e	t

یەکەم پیتی نووسینە ئاساییەکە کە ئیسە s لادەبەین و ژمارە یەك (١) ی بۆ دادەنێین. چونکە یەکەم وشەی سایفەری بووك Book Cipher بە ئیس s دەستپێدەکات، کە بریتییە لە seven.

دووەم پیتی نووسینە ئاساییەکە کە ئییە e لادەبەین و، ژمارە چوار (٤) ی بۆ دادەنێین. چونکە چوارەم وشەی سایفەری بووك Cipher Book بە ئی e دەستپێدەکات، کە بریتییە لە eat.

بۆ پیتەکانی تریش بە هەمان شێوەیە و ئەنجام بەم جۆرە دەردەچێت.

Plain Text = secret

Cipher Text = 142543

بەرنامەیەك بنووسە بۆ بە هیماکردنی بیلێ سایفەر

Write Program to Encryption in Beal Cipher

```
class Beale_Cipher
{
	String cipher="";
	String plain="";
	int[]cipher_array;
	char[]key_array;
	char[] generateKey(String pragraph)
	{
		String key="";
		char[]pragraph_array=pragraph.toCharArray();
		key+=pragraph_array[0];
		for(int i=0;i<pragraph_array.length;i++)
		{
			if(Character.isWhitespace(pragraph_array[i]))// DONT PUT
SEMICOLONE HERE , in jdk 7 not giving error but exception
			{
				key+=pragraph_array[i+1];
			}
		}
		System.out.print("The Key is : "+key);//just for display
		key_array=key.toCharArray();
		System.out.println();
		return key_array;
```

```
}
//_____________________________________________________________
int[]encryption(String plain)
{
        char[]key_array=generateKey("seven crazy termites eat rotten elderberries");
        char[]plain_array=plain.toCharArray();
        cipher_array=new int[plain_array.length];
        for(int k=0;k<plain_array.length;k++)
        {
                for(int j=0;j<key_array.length;j++)
                {
                        if(plain_array[k]==key_array[j])
                        {
                                cipher_array[k]=(j+1);
                                cipher+=(j+1);//just for the print(display)
                                break;
                        }
                }
        }
        System.out.println("The Cipher Text = "+cipher);//just for the print(display)
        return cipher_array;
}
//_____________________________________________________________
String decryption()
{
```

```
            for(int k=0;k<cipher_array.length;k++)
            {
                for(int j=0;j<key_array.length;j++)
                {
                    if(cipher_array[k]==j)
                    {
                        plain+=key_array[(j-1)];
                        break;
                    }
                }
            }
            //System.out.println("The Plain Text = "+plain);
            return plain;
        }
        public static void main(String[]args)
        {
            Beale_Cipher ob=new Beale_Cipher();
        //  ob.generateKey("seven crazy termites eat rotten elderberries");
            ob.encryption("secret");
            System.out.println("The Plain Text Is : "+ob.decryption());
        }
}
```

پلەی فایەر سایفەر

Playfair Cipher

لەم جۆرەی سایفەر دا، وشەیەکی سەرەکیمان هەیە Keyword و، دەبێت وشە سەرەکییەکە Keyword بنووسین لەناو ریزکراوەیەکی (ماتریکس – Matrix) پێنج بە پێنج (٥*٥) دا. هەروەها دەبێت هەر دوو پیتی ئای I و جەی J بخەینە یەك خانەوە One Cell و، دەبێت پیتە دووبارەکانیش لابببەین.

دووای ئەنجامدانی ئەم هەنگاوانەی سەرەوە، نووسینە ئاساییەکە Plain Text دابەش دەکەین بۆ چەند بەشێکی دوو پیتی، واتە دوو دوو جیایان ئەکەینەوە و، لەکوێدا دوو پیتە جیاکراوەکە وەکو یەك وابوو، ئەوا پیتی ئێکس X دەخەینە نێوانیانەوە. هەروەها ئەگەر لە یەکێك لە گرووپەکانی کۆتای دا، تەنها یەك پیتی تیابوو، بەهەمان شێوە، پیتی ئێکس X ی بۆ زیاد دەکەین، بۆ ئەوەی ببێتە دووانی.

هەردوو پیتێکی جیاکراوەی دووانی وەکو چوار لایەك وەردەگرین و، دوو پیتی بەرامبەری ئەم گرووپە دووانی یە دەبێتە سایفەر بۆ دوو پیتەکە.

نموونە //

بە پێی دراوەکانی خوارەوە، پرسیارەکە شیکار بکە، بە ئەلگۆریسمی پلەی فایەر:

Keyword: MANCHESTER

Plain Text: THIS SECRET MESSAGE IS ENCRYPTED

وەلام:

یەکەم: وشە سەرەکی یەکە Keyword لە ریزکراوەیەکی (٥*٥) دا، دادەنێین، دووای لابردنی دووبارەکان:

M	A	N	C	H

E	S	T	R	B
D	F	G	I/J	K
L	O	P	Q	U
V	W	X	Y	Z

دووەم: نووسینە ئاساییەکە Plain Text بۆ گرووپی دوو دووی جیا دەکەینەوە و، ئەگەر پیتی دووبارە هەبوو بۆ گرووپەکان پیتی ئیکس زیاد دەکەین هەتاوەکو دووبارەکان لەیەك جیابکەینەوە و، ئەگەر لە کۆتایشدا یەك پیت مایەوە بەهەمان شێوە، پیتی ئێکس X زیاد دەکەین:

Plain Text: TH IS SE CR ET ME SX SA GE IS EN CR YP TE DX

سێهەم هەر گرووپێکی دوو پیتیٚ وەردەگرین و، بەپێی خشتەکەی دروستمان کرد، سایفەرەکەی دیاری دەکەین، کە هەردوو پیتی گرووپێك شێوەی چوار لایەك دروست دەکات و، هەر پیتی بەرامبەر پیتێکی گرووپەکە دەبێتە سایفەر، بۆ نموونە هەر دوو پیتی TH وەردەگرین کە گرووپی یەکەمە:

M	A	N	C	H
E	S	T	R	B
D	F	G	I/J	K
L	O	P	Q	U
V	W	X	Y	Z

لە باری ئاسۆیی بەرامبەرەکان دیاری دەکەین و، بەمەش پیتی ئێن N دەبێتە سایفەری ئێچ H و، پیتی بی B دەبێتە سایفەری تی T. بەو جۆرە بەردەوام دەبین هەتاوەکو سایفەری هەموو گرووپە دووانی یەکان دیاری دەکەین.

Plain Text: TH IS SE CR ET ME SX SA GE IS EN CR YP TE DX

CipherText:BN FR TS RI SR ED TW FS DT FR TM RI XQ RS GV

تیبینی:

یەکەم: ئەگەر پیتی ئای I و جەی J لە وشە سەرەکییەکەدا هەبوو، ئەوا لەگەڵ یەك دای دەنێین. بۆ نموونە ئەگەر وشە سەرەکییەکە بریتیبێت لە جیتەر Jitter.

J/I	T	E	R	

دووەم:ئەگەر گرووپەکان لە لیواری خشتەکەدا بوو، وەکو CH لە نموونەکەدا، ئەوا بەم جۆرە دەبێت:

C →H

H→M

واتە بۆ پیتی ئێچ H دەگەڕیتەوە بۆ سەرەتا و، بۆ سیش C پیتەکەی تەنیشتی.

سێهەم:ئەگەر پیتی بەرامبەری خانەی J/I بوو، ئەوا ئای یان جەی وەردەگرین، بۆ نموونە بۆ جی سی GC، لە بەرامبەر جی G، ئای I یان جەی J وەردەگرین.

ڤیجنەر سایفەر

Vigenere Cipher

ئەم جۆرەی ئەلگۆریسمی کریپتۆگرافی دەستپێدەکات بە ماتریکسێکی (ریزکراوە – Matrix)ئەلف بێ ی بیست و شەش بە بیست و شەش (٢٦*٢٦)، بەشێوەی زنجیرە، یەکەم ریز Row بە ئەی A دەستپێدەکات و، دووەم ریز بە بی B دەست پێدەکات و، هەروەها.

ڤیجنەر سایفەر پێویستی بە وشەیەکی سەرەکی هەیە Keyword کە نیەر Sender و وەرگر Receiver بیزانن، هەروەها هەر کارەکتەرێکی نامە و پەیامەکە Message (Plain Text) دەکرێت بەیەك Combine لەگەڵ کارەکتەرەکانی وشە سەرەکییەکە Keyword بۆدۆزینەوەی سایفەر Cipher Text.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

یەکەم: بە کۆد کردن

Encryption

١. نامەکە Message دووای لابردنی بۆشاییەکانی Space بنووسە.

٢. لە ژێریدا، وشە سەرەکییەکە Keyword بنووسە و، ئەگەر ژمارەی پیتەکانی کەمتر بوو لە ژمارەی پیتەکانی نامە و پەیامەکە Message، ئەوا پیتەکانی وشەسەرەکییەکە لە سەرەتاوە دووبارە بکەرەوە تا ژمارەی پیتەکانیان یەکسان دەبێت.

٣. ئیستا بەراوردی ستوون Column بۆ ریز Row دەکەین بۆ بەکۆد کردنی پیتەکان.

نموونە:

نامە و پەیام Message:

See Me in Mall

وشەی سەرەکی Keyword:

Infosec

وەلآم:

هەنگاوەکانی سەرەوە جێ بەجێدەکەین:

S	E	E	M	E	I	n	M	a	l	l	نامە Message
I	n	f	o	s	e	c	i	n	f	o	وشەی سەرەکیKeyword
A	r	j	A	w	M	P	U	n	Q	Z	بەکۆدکراو Encrypted

بۆ دیسایفەر

Decryption

١. کەسی وەرگر Receiver وشەسەرەکییەکە Keyword لە ژێر سایفەرەکەدا Cipher (بە کۆد کراوەکە) دادەنێت، کارەکتەر بە کارەکتەر بەرامبەر یەك بن.

٢. ریز Row ی هەر کارەکتەرێکی وشەی سەرەکی وەربگرە و، کارەکتەری بەرامبەرەکەی کە سایفەرە لەو ریزەدا بدۆزەرەوە، و بەرامبەر کارەکتەری سایفەر لەو ریزەدا، لەسەرەوەی خشتەکە Top of Table، دەبێتە یەکەم کارەکتەری نامە Massage، و نووسینە ئاساییەکە.

A	r	j	A	w	M	P	U	n	Q	Z	بەکۆدکراو Encrypted
I	n	f	o	s	e	c	i	n	f	o	وشەی سەرەکیKeyword
S	e	e	M	e	I	n	M	a	l	l	نامە Message

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V

```
X   X Y Z A B C D E F G H I J K L M N O P Q R S T U V W
Y   Y Z A B C D E F G H I J K L M N O P Q R S T U V W X
Z   Z A B C D E F G H I J K L M N O P Q R S T U V W X Y
```

هیلّ سایفەر

Hill Cipher

ئەم ڕێگەیە Method گۆڕینی هێڵی Linear جێ بەجێ دەکات، لەسەر دی پیتی نووسینی ئاسایی D Letters of Plain Text بۆ دەست کەوتن و دروووست کردنی دی پیتی سایفەر D Letters of Cipher Text.

هەروەها هەرنامە و پەیامێك دابەش دەکەین بۆ چەند بلۆکێك Block، کە هەر بلۆکە و دی پیتی D Letters تێدایە، پاشان ڕێکی دەخەینەوە لە ریزکراوە Matrixدا، کە یەك ستوون One Column و دی ریزە D Rows، هەروەها ریزکراوەیەك Matrix دروووست دەکەین و بەکاری دەهێنین کە D*D یە و، ماوەکەی لە سفر بۆ بیست و پێنجە.

تیبینی:

هەر بلۆکە و دەبێت بە یەك ئەرەی کە یەك ستوون One Column و، دی ریزی D Rows.

ئەم دوو یاسە بەکار دەهێنین بۆ بەکۆد کردن و دیسایفەر:

Cipher (Or-Encryption) = Key * Message (Or-Plain Text) Mod 26

Decipher (Message, Plain Text) = Key^{-1}*Cipher Mod 26

نموونە:

وشەی یارمەتی HELP بگۆڕە بۆ وشەیەك کە ڕوون نەبێت و لێی تێنەگەین Encrypt؟ بە بەکارهێنانی ئەم کلیلە؟

$$Key = \begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix}$$

لەبەر ئەوەی کلیلەکە Key پێکهاتووە لە دوو ریز Row بۆیە دەیکەین بە بلۆکی دووی ، واتە HE بلۆکی یەکەم و، LP بلۆکی دووەم، کە دوو بلۆکی دوویمان درووست کرد، ئیستا ئیندێکی هەر یەکێك لە H و E دیاری دەکەین و، لە ماتریێکسێك دا، دای دەنێین و، بەهەمان شێوە بۆ LPیش:

$$M1=\begin{pmatrix} H \\ E \end{pmatrix}=\begin{pmatrix} 7 \\ 4 \end{pmatrix}$$

$$M2=\begin{pmatrix} L \\ P \end{pmatrix}=\begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

یاسای دۆزینەوەی سایفەر بەکار دەهێنین:

$$C=K*M\%26$$

$$C1=\begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix}\begin{pmatrix} 7 \\ 4 \end{pmatrix}=\begin{pmatrix} 3 \\ 3 \\ \end{pmatrix}=\begin{pmatrix} 7 \\ 8 \end{pmatrix}=\begin{pmatrix} H \\ I \end{pmatrix}$$

$$C2=\begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix}\begin{pmatrix} 1 \\ 1 \end{pmatrix}=\begin{pmatrix} 7 \\ 8 \\ \end{pmatrix}=\begin{pmatrix} 0 \\ 1 \\ \end{pmatrix}=\begin{pmatrix} A \\ T \end{pmatrix}$$

دیسایفەر Decipher ئەرکە بۆ خۆتان

بەرنامەیەك بنووسە بۆ بەهێماكردن بە هیلێ سایفەر

Write Program to Encryption Using Hill Cipher

```
import java.awt.*;
import java.awt.event.*;
import javax.swing.*;
import javax.swing.GroupLayout;
import javax.swing.LayoutStyle;
import javax.swing.border.*;
/*
 * Created by JFormDesigner
 */
/**
 * @author Hemn Barznji
 */
public class HillHill extends JFrame {
          static char
[]array={'A','B','C','D','E','F','G','H','I','J','K','L','M','N','O','P','Q','R','S','T','U','V','W','X','Y','Z'};
        char []array2={'a','b','c','d','e','f','g','h','i','j','k','l','m','n','o','p','q','r','s','t','u','v','w','x','y','z'};
          static char
[]array1={'A','B','C','D','E','F','G','H','I','J','K','L','M','N','O','P','Q','R','S','T','U','V','W','X','Y','Z'};
   int number[]={1,3,5,7,9,11,15,17,19,21,23,25};
   static char []encryptArray=new char[26];
   static char [][]array3;
          static char []encryptArray1;
   static String print;
```

```
    public HillHill() {
        initComponents();
        setVisible(true);
    }

    private void button13ActionPerformed(ActionEvent e) {
        // TODO add your code here
        Hill();
    }
    private void button14ActionPerformed(ActionEvent e) {
        // TODO add your code here
        setVisible(false);
    }

    private void initComponents() {
        // JFormDesigner - Component initialization - DO NOT MODIFY  //GEN-
BEGIN:initComponents
        panel13 = new JPanel();
        panel14 = new JPanel();
        textField3 = new JTextField();
        textField4 = new JTextField();
        textField5 = new JTextField();
        textField6 = new JTextField();
        scrollPane14 = new JScrollPane();
        textArea12 = new JTextArea();
```

```
scrollPane15 = new JScrollPane();

textArea13 = new JTextArea();

button13 = new JButton();

button14 = new JButton();


//======== this ========

setTitle("Hill");

Container contentPane = getContentPane();


//======== panel13 ========

{

        panel13.setBorder(LineBorder.createBlackLineBorder());

        panel13.setBackground(Color.lightGray);


        //======== panel14 ========

        {

                panel14.setBorder(new
TitledBorder(UIManager.getBorder("CheckBox.border"), " Matrix", TitledBorder.CENTER,
TitledBorder.TOP));

                panel14.setBackground(Color.lightGray);


                GroupLayout panel14Layout = new GroupLayout(panel14);

                panel14.setLayout(panel14Layout);

                panel14Layout.setHorizontalGroup(

                        panel14Layout.createParallelGroup()

                                .addGroup(panel14Layout.createSequentialGroup()

                                        .addContainerGap()
```

```
        .addGroup(panel14Layout.createParallelGroup(GroupLayout.Alignment.TRAILING)
                                                    .addComponent(textField3,
GroupLayout.DEFAULT_SIZE, 53, Short.MAX_VALUE)
                                                    .addComponent(textField5,
GroupLayout.DEFAULT_SIZE, 53, Short.MAX_VALUE))

        .addPreferredGap(LayoutStyle.ComponentPlacement.UNRELATED)

        .addGroup(panel14Layout.createParallelGroup()
                                                    .addComponent(textField6,
GroupLayout.DEFAULT_SIZE, 60, Short.MAX_VALUE)
                                                    .addComponent(textField4,
GroupLayout.DEFAULT_SIZE, 60, Short.MAX_VALUE))
                                                .addGap(21, 21, 21))
                                );
                                panel14Layout.setVerticalGroup(
                                        panel14Layout.createParallelGroup()
                                                .addGroup(panel14Layout.createSequentialGroup()
                                                        .addContainerGap()

        .addGroup(panel14Layout.createParallelGroup(GroupLayout.Alignment.BASELINE)
                                                    .addComponent(textField3,
GroupLayout.PREFERRED_SIZE, GroupLayout.DEFAULT_SIZE, GroupLayout.PREFERRED_SIZE)
                                                    .addComponent(textField4,
GroupLayout.PREFERRED_SIZE, GroupLayout.DEFAULT_SIZE, GroupLayout.PREFERRED_SIZE))

        .addPreferredGap(LayoutStyle.ComponentPlacement.RELATED)

        .addGroup(panel14Layout.createParallelGroup(GroupLayout.Alignment.BASELINE)
                                                    .addComponent(textField6,
```

```
GroupLayout.PREFERRED_SIZE, GroupLayout.DEFAULT_SIZE, GroupLayout.PREFERRED_SIZE)
                                                .addComponent(textField5,
GroupLayout.PREFERRED_SIZE, GroupLayout.DEFAULT_SIZE, GroupLayout.PREFERRED_SIZE))

        .addContainerGap(GroupLayout.DEFAULT_SIZE, Short.MAX_VALUE))
                        );
                }

                //======== scrollPane14 ========
                {
                        scrollPane14.setBorder(new
TitledBorder(UIManager.getBorder("CheckBox.border"), "Input File", TitledBorder.CENTER,
TitledBorder.TOP));
                        scrollPane14.setBackground(SystemColor.inactiveCaption);

                        //---- textArea12 ----
                        textArea12.setBackground(Color.white);
                        scrollPane14.setViewportView(textArea12);
                }

                //======== scrollPane15 ========
                {
                        scrollPane15.setBorder(new
TitledBorder(UIManager.getBorder("CheckBox.border"), "Output File", TitledBorder.CENTER,
TitledBorder.TOP));
                        scrollPane15.setBackground(SystemColor.inactiveCaption);
                        scrollPane15.setViewportView(textArea13);
                }
```

```
        //---- button13 ----
        button13.setText("Encryption");
        button13.setFont(new Font("Tahoma", Font.BOLD, 12));
        //button13.setBackground(Color.black);
        button13.addActionListener(new ActionListener() {
            @Override
            public void actionPerformed(ActionEvent e) {
                button13ActionPerformed(e);
            }
        });

        //---- button14 ----
        button14.setText("Eixt");
        button14.setFont(new Font("Tahoma", Font.BOLD, 12));
        //button14.setBackground(Color.black);

        GroupLayout panel13Layout = new GroupLayout(panel13);
        panel13.setLayout(panel13Layout);
        panel13Layout.setHorizontalGroup(
            panel13Layout.createParallelGroup()
                .addGroup(panel13Layout.createSequentialGroup()
                    .addGroup(panel13Layout.createParallelGroup()

.addGroup(panel13Layout.createSequentialGroup()
                                                .addContainerGap()
                                                .addComponent(panel14,
```

```
GroupLayout.DEFAULT_SIZE, GroupLayout.DEFAULT_SIZE, Short.MAX_VALUE))

        .addGroup(panel13Layout.createSequentialGroup()

                                                .addGap(38, 38, 38)

        .addGroup(panel13Layout.createParallelGroup(GroupLayout.Alignment.TRAILING, false)

                                                .addComponent(button14,
GroupLayout.Alignment.LEADING, GroupLayout.DEFAULT_SIZE, GroupLayout.DEFAULT_SIZE,
Short.MAX_VALUE)

                                                .addComponent(button13,
GroupLayout.Alignment.LEADING, GroupLayout.DEFAULT_SIZE, GroupLayout.DEFAULT_SIZE,
Short.MAX_VALUE))

                                                .addGap(9, 9, 9)))

                                        .addGap(18, 18, 18)

        .addGroup(panel13Layout.createParallelGroup(GroupLayout.Alignment.LEADING, false)

                                                .addComponent(scrollPane15)

                                                .addComponent(scrollPane14,
GroupLayout.DEFAULT_SIZE, 259, Short.MAX_VALUE))

                                        .addContainerGap())

                );

                panel13Layout.setVerticalGroup(

                        panel13Layout.createParallelGroup()

                                .addGroup(panel13Layout.createSequentialGroup()

                                        .addContainerGap()

        .addGroup(panel13Layout.createParallelGroup(GroupLayout.Alignment.TRAILING)

                                                .addComponent(panel14,
GroupLayout.PREFERRED_SIZE, GroupLayout.DEFAULT_SIZE, GroupLayout.PREFERRED_SIZE)

                                                .addComponent(scrollPane14,
```

```
GroupLayout.PREFERRED_SIZE, 75, GroupLayout.PREFERRED_SIZE))
                                        .addGroup(panel13Layout.createParallelGroup()

        .addGroup(panel13Layout.createSequentialGroup()
                                                .addGap(18, 18, 18)
                                                .addComponent(scrollPane15,
GroupLayout.PREFERRED_SIZE, 66, GroupLayout.PREFERRED_SIZE))

        .addGroup(panel13Layout.createSequentialGroup()
                                                .addGap(11, 11, 11)
                                                .addComponent(button13)
                                                .addGap(18, 18, 18)
                                                .addComponent(button14)))
                                        .addContainerGap(118, Short.MAX_VALUE))
                );
        }

        GroupLayout contentPaneLayout = new GroupLayout(contentPane);
        contentPane.setLayout(contentPaneLayout);
        contentPaneLayout.setHorizontalGroup(
                contentPaneLayout.createParallelGroup()
                        .addGroup(GroupLayout.Alignment.TRAILING,
contentPaneLayout.createSequentialGroup()
                                .addContainerGap(GroupLayout.DEFAULT_SIZE,
Short.MAX_VALUE)
                                .addComponent(panel13, GroupLayout.PREFERRED_SIZE,
GroupLayout.DEFAULT_SIZE, GroupLayout.PREFERRED_SIZE)
                                .addContainerGap())
```

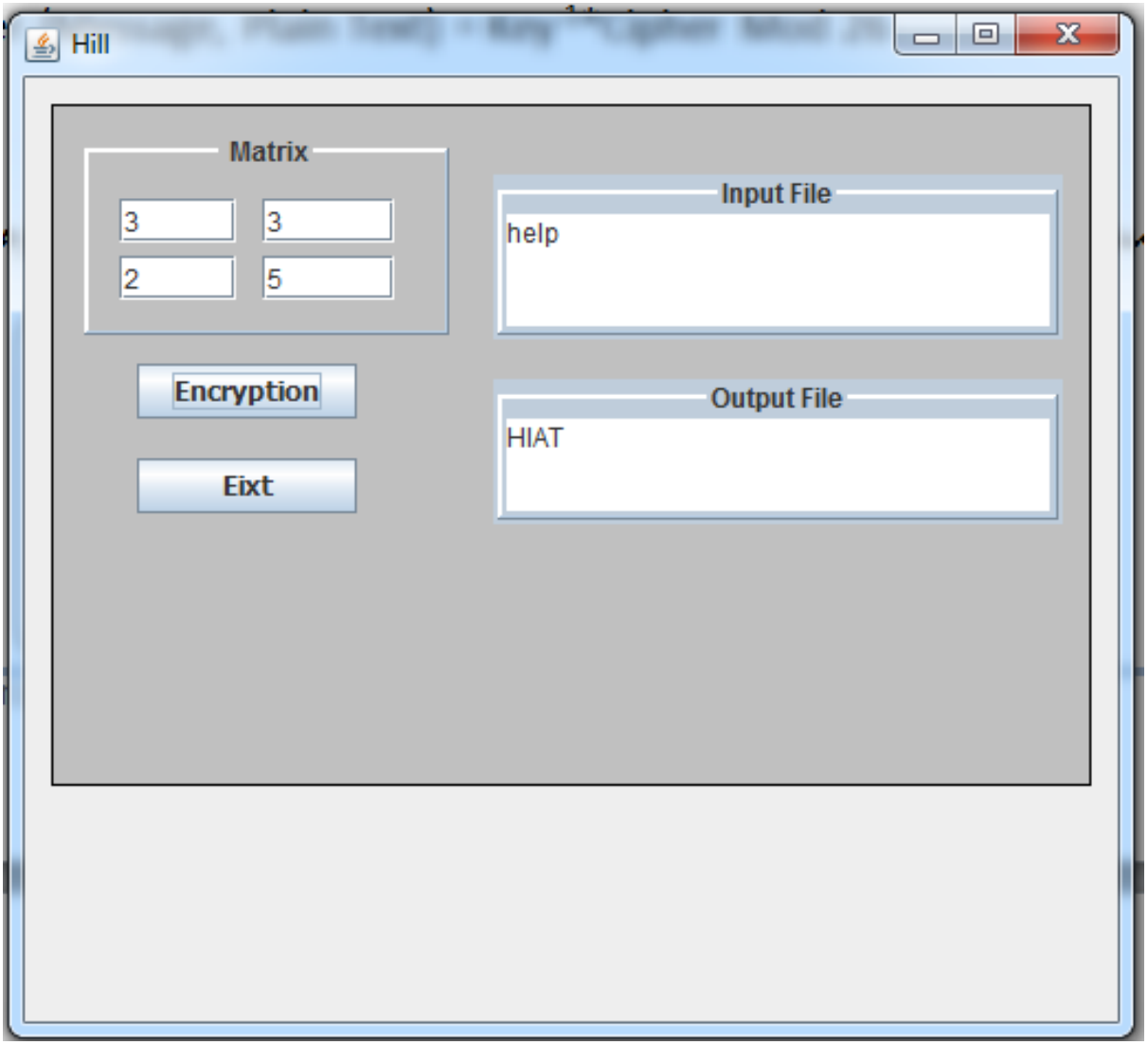
```
                );
                contentPaneLayout.setVerticalGroup(
                        contentPaneLayout.createParallelGroup()
                                .addGroup(GroupLayout.Alignment.TRAILING,
contentPaneLayout.createSequentialGroup()
                                        .addContainerGap(GroupLayout.DEFAULT_SIZE,
Short.MAX_VALUE)
                                        .addComponent(panel13, GroupLayout.PREFERRED_SIZE,
GroupLayout.DEFAULT_SIZE, GroupLayout.PREFERRED_SIZE)
                                        .addGap(107, 107, 107))
                );
                pack();
                setLocationRelativeTo(getOwner());
                // JFormDesigner - End of component initialization  //GEN-END:initComponents
        }

//////////////////////////////////////////////////////////////////hill
char ch;
int[][]letter=new int[2][1];
int d;
int data=0;
String stE="";
char[] alpha= {'A','B','C','D','E','F','G','H', 'I','J','K','L','M', 'N','O','P','Q','R','S','T','U','V','W','X','Y','Z'};


public String encrypt(String st1,int[][]key)
{
```

```
            String st=st1.toUpperCase();
            if(st.length()%2!=0)
                st+="X";
            char [] array=st.toCharArray();
            for(int i=0;i<array.length;i++)
                {
                    if(array[i]!=' ')
                    {
                        for(int j=0;j<1;j++)
                        {
                            letter[d][0]=findIndex(array[i]);
                            d++;
                            if(d==2)
                            {
                                stE+=multiPlication(key,letter);
                                d=0;
                            }
                        }
                    }
                    else
                    {
                        stE+=" ";
                    }
              }
        return stE;
}
```

```
//////////////////////////////////////////////////////////////////////////
int findIndex(char ch)
{
	int num=0;
	for(int j=0;j<alpha.length;j++)
				{
					if(ch==alpha[j])
					{
						num=j;
					}
			}
			return num;
}
//////////////////////////////////////////////////////////////////////////
String findChar(int  index)
{
	String st ="";
	for(int j=0;j<alpha.length;j++)
				{
					if(index==j)
					{
						st+=alpha[j];
					}
			}
			return st;
}
```

```
//////////////////////////////////////////////////////////////////////////
String multiPlication(int[][]key,int letter[][])
{
        String st="";
        for(int i=0;i<key.length;i++)
                {
                        for(int j=0;j<2;j++)
                        {
                                data=data+(key[i][j]*letter[j][0]);
                        }
                        st+=findChar(data%26);
                        data=0;
                }

        return st;
}
public void Hill(){
        int A=Integer.parseInt(textField3.getText());
   int B=Integer.parseInt(textField4.getText());
        int C=Integer.parseInt(textField5.getText());
        int D=Integer.parseInt(textField6.getText());

    int[][]key =new int[2][2];
```

```
   key[0][0]=A;
   key[0][1]=B;
   key[1][0]=C;
   key[1][1]=D;
String text=textArea12.getText();
textArea13.append(encrypt(text,key));
        }

        // JFormDesigner - Variables declaration - DO NOT MODIFY  //GEN-BEGIN:variables
        private JPanel panel13;
        private JPanel panel14;
        private JTextField textField3;
        private JTextField textField4;
        private JTextField textField5;
        private JTextField textField6;
        private JScrollPane scrollPane14;
        private JTextArea textArea12;
        private JScrollPane scrollPane15;
        private JTextArea textArea13;
        private JButton button13;
        private JButton button14;
        // JFormDesigner - End of variables declaration  //GEN-END:variables
                public static void main(String[]args)
                {
                        new HillHill();      }
}
```


Hill
Matrix
3
3
2
5
Input File
help
Encryption
Output File
HIAT
Eixt

پادەکانی یەك کاتی

One Time Pads

لەم رێگەیەدا، هەموو پیتەکانی نووسینە ئاساییەکە Plain Text دەنووسین لە خشتەیەکدا، بێ لابردنی دووبارەکان ، پاشان ژمارەی ئیندێکسی هەر پیتێك لە ژێر پیتەکەدا، دەنووسین، هەروەها پیتەکانی وشە سەرەکییەکەش لە خشتەکەدا دەنووسین و، ژمارەی هەر ستوونێك کۆدەکەینەوە و، مۆدەکەی وەردەگرین، بەمەش سایفەری هەر پیتێکمان دەست دەکەوێت، بۆ نموونە:

Plain Text = the British Have Fifty Tanks

Keyword = She Loves Him So Very Much Now.

	T	h	e	B	r	i	t	i	s	h	h	a	v	e
	19	7	4	1	17	8	19	8	18	7	7	0	21	4
	S	h	e	L	o	v	e	s	H	i	m	S	o	v
	18	7	4	11	14	21	4	18	7	8	12	18	14	21
Add	37	14	8	12	31	29	23	26	25	15	19	18	35	25
Mod	11	14	8	12										
New Letter														

جێگۆرکێ ی ستوونی

Columnar Transposition

ئەم جۆرەی بە کۆد کردنی نووسین و نامە و پەیامە ئاساییەکان Plain Text، جیاوازە لە ڕێگەکانی تر لە هەنگاوەکانی کار کردن و دروست کردنی دا و، بەم هەنگاوانەی خوارەوە دەتوانین بە کۆد کردن Encryption ئەنجام بدەین:

١. ڕێکخستنەوەی نامە و پەیامەکە لە ریزکراوە Array دوو ڕەهەندی و دوو دووری 2 Dimension دا.

٢. ژمارەی ریزەخانەی ئاسۆیی Row و، ستوون Column پشت دەبەستێت بە درێژی نامە و پەیامەکە.

٣. ئەگەر درێژی نامەکە بکاتە ٣٠ کارەکتەر ئەوا ژمارەی ریز و ستوون دەکاتە: ١٥*٢، ٢*١٥، ١٠*٣، ٣*١٠، ٥*٦، ٦*٥.

٤. ئەگەر دێژی نامەیەك بکاتە ٢٩ کارەکتەر ئەوا پیتێك لە کۆتای دا، زیاد دەکەین.

نموونە / ئەگەر نامەکە ریتیبێت لە Hello World و، کلیلەکەش بریتیبێت لە ٢و١.

Plain Text = Hello World

Key = (2,1)

وەڵام:

ژمارەی پیتەکانی نووسینە ئاساییەکە Plain text دە (١٠) یە، بۆیە ژمارەی ریز و ستوونەکان دەکاتە: ٢*٥ یان ٥*٢، بەڵام ١*١٠ یان ١٠*١ ناگونجێت و وەری ناگرین.

ئیستا نامەکە دەکەین بە ریزکراوەیەکی دوو دووری 2D Array، دوو ستوون بە ٥ ریز.

	Column 1	Column 2
Row 1	H	e
Row 2	l	l
Row 2	o	w
Row 4	o	r
Row 5	l	d

لەبەر ئەوەی بە گوێرەی ژمارەی کلیلەکان بریار دەدەین کام ستوونە Column یەکەم جار بنووسرێت، و کام ستوونە دووەم جار و، کام ستوونە سێهەم جار و، بەو شێوەیە، وە لێرەدا ژمارەی کلیلەکان دووە، بۆیە کردمانە دوو ستوون و، بە گوێرەی کلیلەکە ستوونی دووەم دەنووسین و، پاشان ستوونی یەکەم، بە دووای دا.

Plain Text = Hello World

Key = (2,1)

Cipher = elwrd hlool

نموونەی دووەم: ئەگەر زانیاریییەکان بەم شێوەیەی لای خوارەوە بێت، ئەوا بە بەکارهێنانی رێگەی جێگۆرکێ ی تووونەکان، نامەکە بگۆرە بۆ شێوەیەك کە نە خوێندرێتەوە:

Plain Text = HLLO WORLD

Keys = (4,1,2,5,3)

وەلام:

ژمارەی پیتەکانی نامەکە ١٠ پیتە و، ئەمەش لە ٢*٥ یان ٥*٢ دروست دەبێت و، ئێمە ٥*٢ وەردەگرین، واتە ٥ ستوون Column و، دوو ریز Row. چونکە پێنج کلیلمان هەیە و، ژمارە کلیلەکان ئاماژەیە بۆ ژمارەی ستوونەکان.

	Column 1	Column 2	Column 3	Column 4	Column 5
Row 1	h	e	l	l	o
Row 2	w	o	r	l	d

بە گوێرەی کلیلە دراوەکە، ئەنجامی بە کۆد کردن بەم جۆرە دەبێت:

Plain Text = HLLO WORLD

Keys = (4,1,2,5,3)

Cipher = ll hw eo od lr

نموونەی سێهەم: نامەی هەمان نموونەکەی پێشوو Hello Word بگۆرە بۆ کۆد Cipher بە بەکارهێنانی کلیلەکانی ٢١٣.

دووجار جێگۆرکێ کردنی ستوون

Double Columnar Transposition

ئەم ڕێگەیەی بە کۆد کردن، وەکو ڕێگەی پێشوو وایە، تەنها لەوەدا جیاوازە کە دوو جار کرداری جێگۆرکێ کردن دووبارە دەبێتەوە و، دووجار جێ گۆرکێ ڕوودەدات، جارێکیان بە گوێرەی کلیلی یەکەم و، جاری دووەم جێ گۆر کێ کردنە بە ئەنجامەکە بە بەکارهێنانی کلیلی دووەم.

نموونە: ئەم نامە و پەیامەی خوارەوە بگۆرە بۆ کۆد، بە بەکارهێنانی دوو کلیلی جیاواز، کلیلی یەکەم و کلیلی دووەم:

Plain Text = Hello World

First Key = (2,1,3) & Second Key = (3,2,1).

وەڵام:

لە بەر ئەوەی نامەکە ١٠ پیتە و، بە پێی کلیلی یەکەمیش کە سی کلیلە، ٢ و ١ و ٣ یە، بۆیە دەبێت بیکەینە سێ ستوون Column و، بۆ ئەمەش ٣ لێکدانی ژمارەیەکی دەکەین تا بکاتە ١٠ یان گەورەتر لە ١٠، چونکە کە گەورەتر بوو خانە زیادە بەتاڵەکان بە پیتی ئیکس پر دەکەینەوە، بەڵام گەر بچووکتر بوو، ئەوا ناگونجێت. چونکە نامە و پەیامە ئاساییەکە جێگەی نابێتەوە تیایدا، بۆیە ٣*٤ وەردەگرین و، بەمەش ١٢ خانەمان دەبێت و، دوو خانەی کۆتایی بە ئیکس پر دەکەینەوە:

	Column 1	Column 2	Column 3
Row 1	h	e	l
Row 2	l	o	w
Row 3	o	r	l
Row 4	d	x	x

به پێی کلیلە دراوەکەی یەکەم، یەکەم بە کۆد کردن First Cipherدەکاتە:

First Cipher = eorx hlod lwlx

پاشان بە گوێرەی کلیلی دووەم، دووەمین جێگۆرکێ ئەنجام دەدەین، کە لە سەر ئەنجامەکەی پێشوو، کارەکە دەکەین بە دووبارە کردنەوەی هەنگاوەکان:

	Column 1	Column 2	Column 3
Row 1	e	o	r
Row 2	x	h	l
Row 3	o	d	l
Row 4	w	l	x

بە گوێرەی کلیلی دووەم، دووەم سایفەر دەکاتە:

Second Encryption = rllx ohdl exow

تیبینی:

1. **لەوانەیە کارەکتەر، بەکار بهێنرێت بۆ پیشاندانی کلیلەکان.**
2. **ئەگەر کلیلەکان جیاواز بوو، دەگونجێت و، ئیمە گوێ نادەین بەو جیاوازییە و، لەسەر کلیلەکان کار دەکەین.**
3. **بە کۆد کردنەوەی دووەم، بە کۆد کردنی یەکەم، واتە ئەنجامی یەکەمە و، بە کۆدمان کردووە.**

بەشی چوارەم

دی ئی ئێس، ئەی ئی ئێس و ئارِ ئێس ئەی

DES, AES & RSA

بەهێماکردنی پێوانەیی زانیاری

Data Encryption Standard (DES)

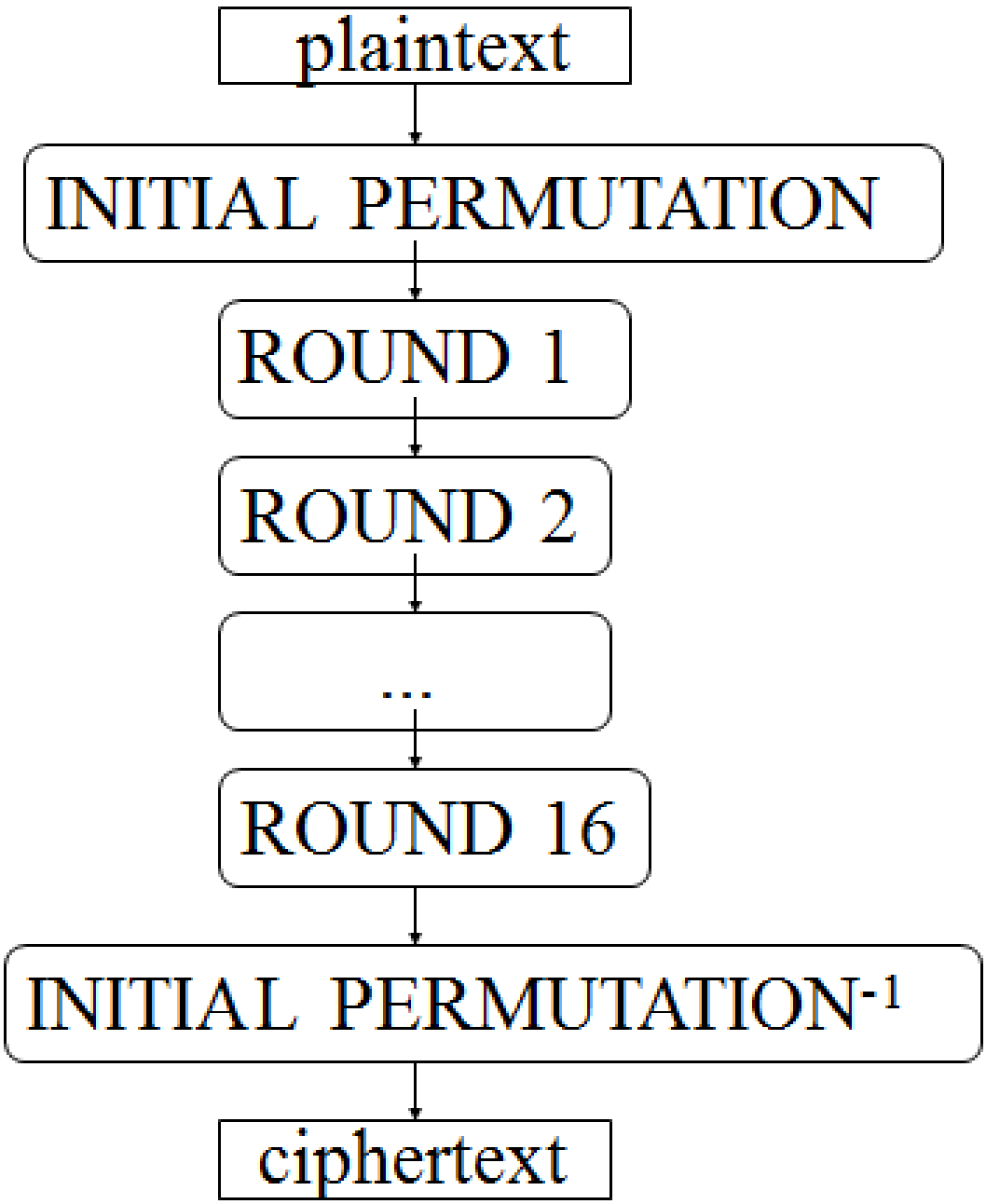
بەهێماکردنی پێوانەیی زانیاری Data Encryption Standard (DES): ئەلگۆریسمی بەهێماکردنە Encryption Algorithm کە زانیاری ئاسایی و خوێنراوە دەکاتە هێما، بە بەکارهێنانی ٥٦-بت، بەشێوەیەکی هەرەمەکی کلیلی هاوتا Symmetric Key دروست دەکات، ئەلگۆریسمی دی ئی ئیس DES دروستکراوە لە لایەن کۆمپانیای ئی بی ئێم IBM Company و حکومەتی ویلایەتە یەکگرتووەکان پێکەوە، دی ئی ئیس لە ئەلگۆریسمی جۆری کۆمەڵە (بلۆك) Blockیە .

چاوپیاخشانیکی گشتی Overview

ئەلگۆریسیمی دی ئی ئیس پێکهاتەیەکی ئالۆز و وردی هەیە، دوو قاڵبی بنچینەیی دروستکردنی بەهێماکردن Encryption: سایفەری خستنە جێ Sustitution Cipher ((کە سایفەری جۆگەلەییە Stream Cipher کە کاردەکات لەسەر نووسینی ئاسایی بەهۆی ئالۆگۆری کارەکتەرەکان لەگەڵ دانەی نوێی ئەلف بێ)) لەگەڵ سایفەری جێگۆرکێ Transposition Cipher((کە سایفەری بلۆك Block Cipher کە کاردەکات لەسەر نووسینی ئاسایی بە گۆرینی شوێنی کارەکتەرەکان Position of Character، لە نووسینی ئاسایی Plain Text)). بەهێزی ئەم ئەلگۆریسمە لە دووبارەکردنەوە و جیبەجێکردنی ئەو دوو تەکنیکەدایە، بۆ هەموو ١٦ سورەکە.

ئەم ئەلگۆریسمە دەست دەکات بە گۆرینی نووسینی ئاسایی Plain Text بۆ هێما Cipher، بە بەکارهێنانی دارشتگە و قاڵبی Block ٦٤ بتی لە نووسینی ئاسایی Plain Text، کلیلەکەش The Keyشەست و چوار (٦٤) بتە.

بەڵام لە راستیدا، هەر ٥٦-بتێك گونجاوە بۆ کارەکە و، هەشت بیتەکەی تر بەکاردەهێنرێن وەکو ژمارەیی پشکنین Check Digit و، کاریگەرییان نابێت لەسەر کرداری بەهێما کردن Encryptionلە جێبەجێکردنی ئاسایی دا. گونجاوە بۆ ئەوەی بەکارهێنەر کلیلەکە بگۆرێت لە هەر کاتێکدا.

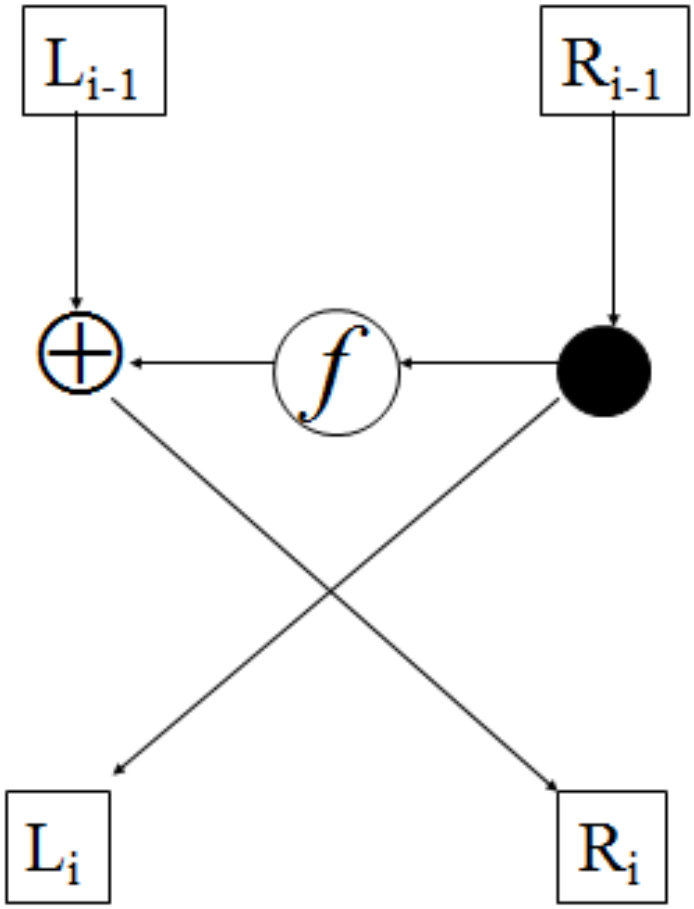


یەك سوور

One Round

لە هەر سوورێکدا، ٦٤ بتەکە دابەش دەبێت بۆ لای چەپ Left و لای راست Right، نیوەیی لای راست Right Half بە کرداریی Function ئیف Fدا دەرووات، لەگەڵ کلیلەکەدا تێکەڵ Mixed With Key دەبێت، پاشان نیوەی لای راست Right Half زیاد دەبێت Add بۆ نیوەی لای چەپ Left Half،

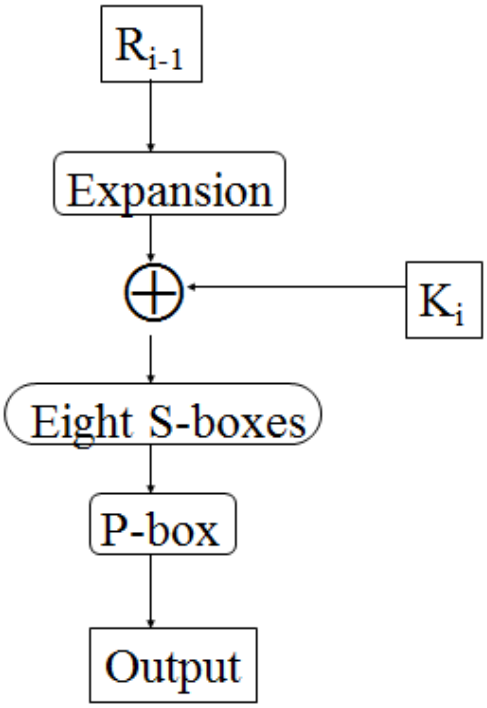
پاشان نیوەکان ئالۆگۆر دەبن، جگە لە سووری کۆتایی کە ئالۆگۆر کردنی نیوەکان رووندەدات.



لە ناوەوە

Inside

پاشان لە ناوەوە، چەندین کار رووەدات. لای راست Right Side فراوان دەبێت Expand، لە ٣٢ بتەوە بۆ ٤٨ بت، کە بەکارهێنانەوەی هەندێك لە بتەکانە، پاشان ٤٨ بت کلیلی بۆ زیاد دەبێت Add 48 Bits of Key، کە بە گوێرەیی خشتە هەڵدەبژێردرێت، دوواتر سنووقەکانی ئیس S- Boxs هەموو کۆمەڵەیەکی ٦ بتی کەم دەکەنەوە بۆ ٤ بت، سنووقی پیش P-Box ئالۆگۆری ٣٢ بتەکان دەکەن.



پێچەوانە کردنەوەکان

Inverses

هاوکێشەیی سوری ئای Equation of Round I **بریتییە لە :**

$$L_i = R_{i-1}$$

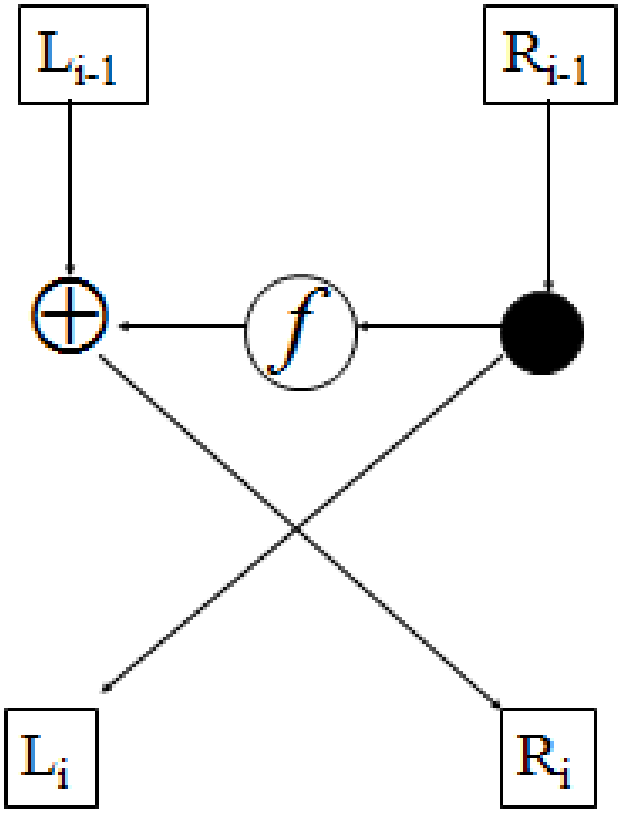
$$R_i = L_{i-1} \oplus f\left(R_{i-1}\right)$$

یان بە مانا و شێوەیەکی تر :

$$R_{i-1} = L_i$$

$$L_{i-1} = R_i \oplus f\left(L_i\right)$$

لە بەر ئەوە گۆرینی بەهێماکراو بۆ نووسینی ئاسایی Decryption بەهەمان شێوەی کرداری بە کۆد کردنە Encryption. دووا سوور ئالّو گۆر نەکراوە:



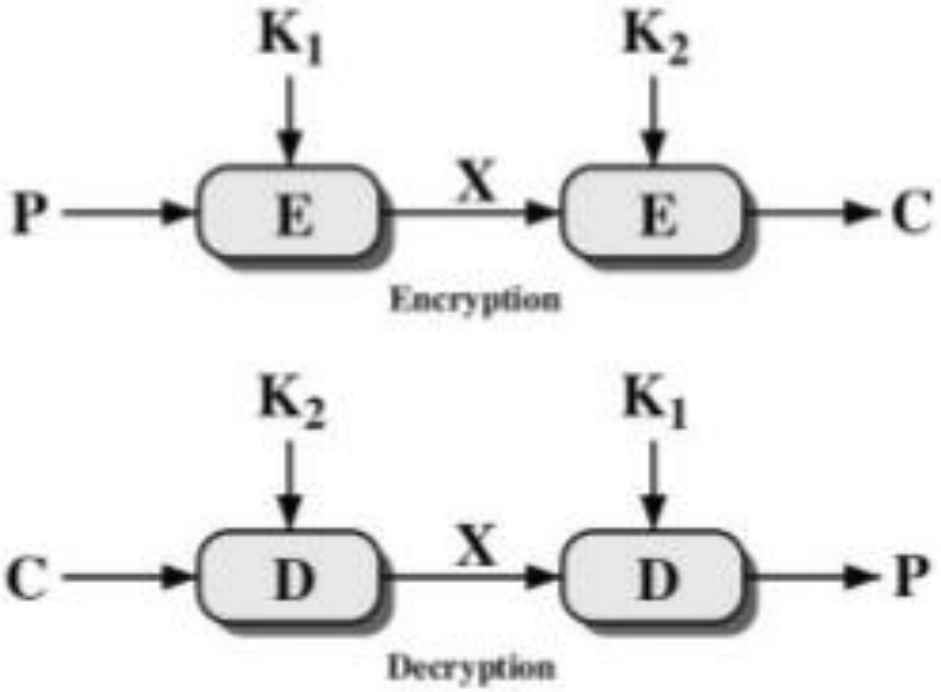
دووانە دی ئی ئیس

Double DES

بۆ چارەسەرکردنی نارەحەتی و کێشە و گرفتەکان، هەندێك لە توێژەران پێشنیاری بەکارهێنانی دووانە بەهێماکردنیان Double Encryption کرد، بۆ زیاتر کردنی ئاسایشیی و نهێنی. دووانە بە هێماکردنکەش The Double Encryption لەسەر بنچینەیی ئەم رێگەیەی خوارەوە کاردەکات. دوو کلیك 2 Keys وەردەگرێت، واتە کلیلی یەکەم K1 و کلیلی دووەم K2، پاشان جیبەجێکردنی دوو بە هێماکردن 2 Encryption، یەکەم لەسەر ئەوەی تر E(K2, E(K1,m))، لە رووانگەی تیۆرییەوە، تێکشکاندنی ئەم رێبازی بەهێماکردنە زۆر قورس و گرانە، وەك دەزانین هەلبژاردنی دوو قوفل باشترە لە یەك،

پاراستنی دوو قووفڵ زیاتره له یەك.

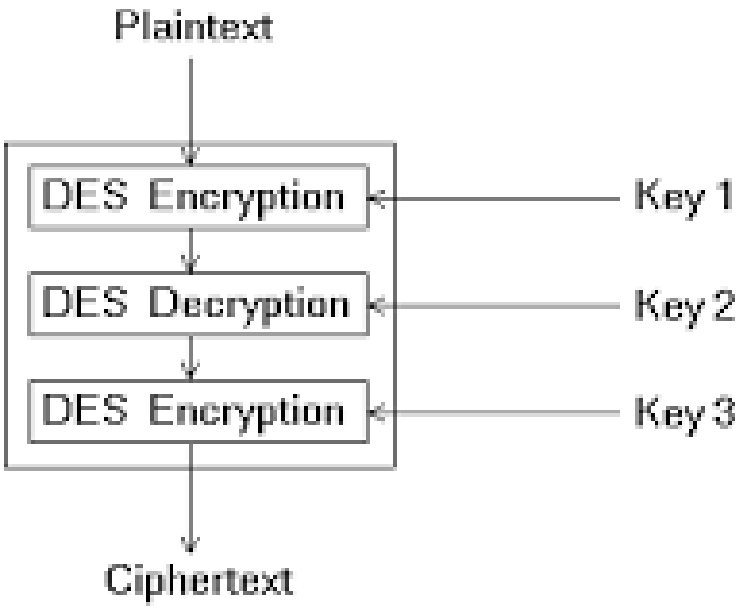
بەڵام بە داخەوە، ئەم گریمانەیە نادروستە، مێرکڵ Merkle و هیڵمان Hellmanپیشانیان دا کە دوو بەهێماکردن باشتر نی یە لەیەك بە هێماکردن.



سیانە دی ئی ئێس

Triple DES

دی ئی ئیسی سیانی 3DES، کە بە Triple DES ناودەبرێت، لە دی ئی ئێسەوە DES بەرهەم هاتووە و پەرە پێدراویی دی ئی ئێسە، بە بەکارهێنانی کلیلی ٦٤ بتی 64-Bit Key، کە پێکهاتووە لە ٥٦ بتی بنچینەیی چالاك و، ٨ بتی تەوازن، لە دی ئی ئیسی سیانی 3DESدا، سێ (٣) جار بەهێماکردنی دی ئی ئیس DES Encryption بەسەر نووسینی ئاسایی Plain Textدا جیبەجێدەبێت. نووسینی ئاسایی Plain Textدەکریتە هێما لەگەل کلیلی ئەی A، پاشان دەگیردریتەوە بۆ شێوەی ئاسایی بەهۆی کلیلی بی B، جارێکی تر دەکریتەوە بە هێما بە بەکارهێنانی کلیلی سی C. دی ئی ئێسی سیانی لە جۆری ئەلگۆریسمی بەهیماکردنی داڕشتگەیی ((پارچەیی/قاڵبی)) یە Block Encryption Algorithm.



پێوەری بەهێماکردنی پێشکەوتوو

Advanced Encryption Standard

ئەلگۆریسمی دی ئی ئێس DES Algorithm تێکشکێنرا و، دێرەکانی پیشان درا و خرایە روو، بۆیە ئیتر دوو چاری گرفتی پاراستن بوویەوە، هەروەها سیانە دی ئی ئێس Triple DES–یش خاوە Slow بۆیە دەبێت ئەلگۆریسمێکی تر هەبێت لە داهاتوو تا کارەکانمان بە هۆیەوە جیبەجێبکەین. ئەویش ((پێوەری بە هێماکردنی پێشکەوتووە Advanced Encryption Standard (AES))، ئەم ئەلگۆیسمی ئەی ئی ئێس AES ـــە لە ساڵی ١٩٩٧ دا، راگەیەنرا. ئەگەرچی لە مانگی ٨ ی ١٩٩٨ دا، پانزە ئەلگۆریسم پالێوران، بەلام لە مانگی ٨ ی ١٩٩٩دا، تەنها ٥ دانەیان گەیشتنە کۆتایی.تا لە ساڵی ٢٠٠٠دا، رین – دۆڵ هەلبژێردرا.

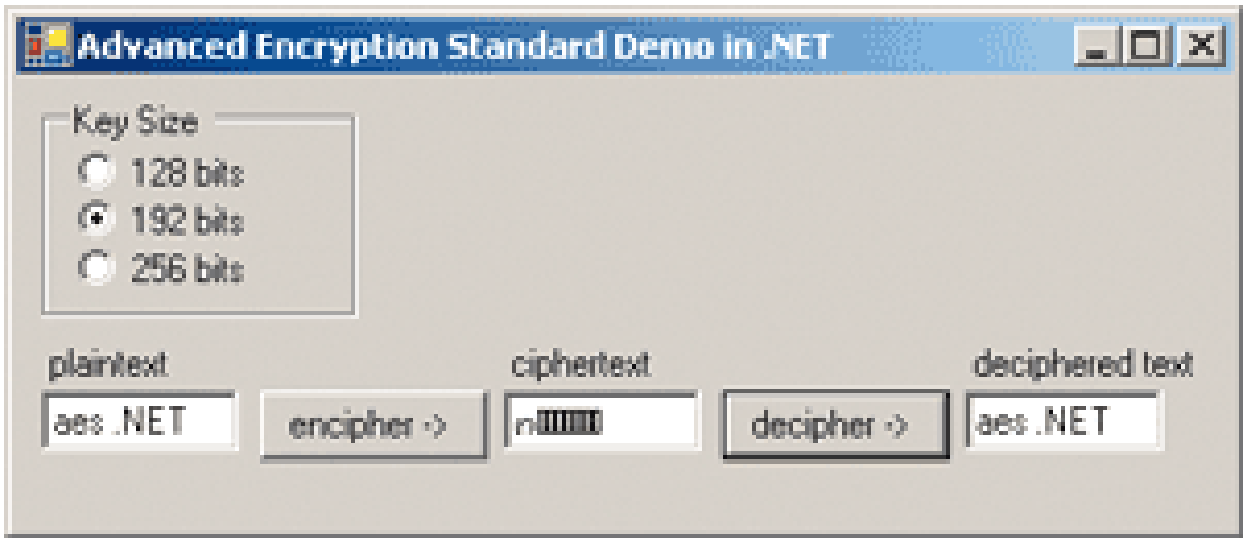
پێوەری بەهێماکردنی پێشکەوتوو Advanced Encryption Standard، بەهێما کردنێکی نوێ و، بەهێزە، کە ئەلگۆریسمی رین-دۆڵ Rijndaelـە، ئەم ئەلگۆریسمە گەشەی پێدراوە لەلایەن Developed جوان دایمن Joan Daemen و ڤنسنت ریجمێن Vincent Rijmen کە دوو کەسی بەلجیکین، ئەم ئەلگۆریسمە کۆچکردنێکبوو Displace بە دی ئی ئیس ئیکس DESX و 3DES، واتە ئەو دووانەی لادا و جێگەی گرتنەوە. ئەی ئی ئێس توانای بەکارهێنانی کلیلی ١٢٨-بتی، ١٩٢- بتی و ٢٥٦-

بتی هەیە.

سوودەکانی

Benefits

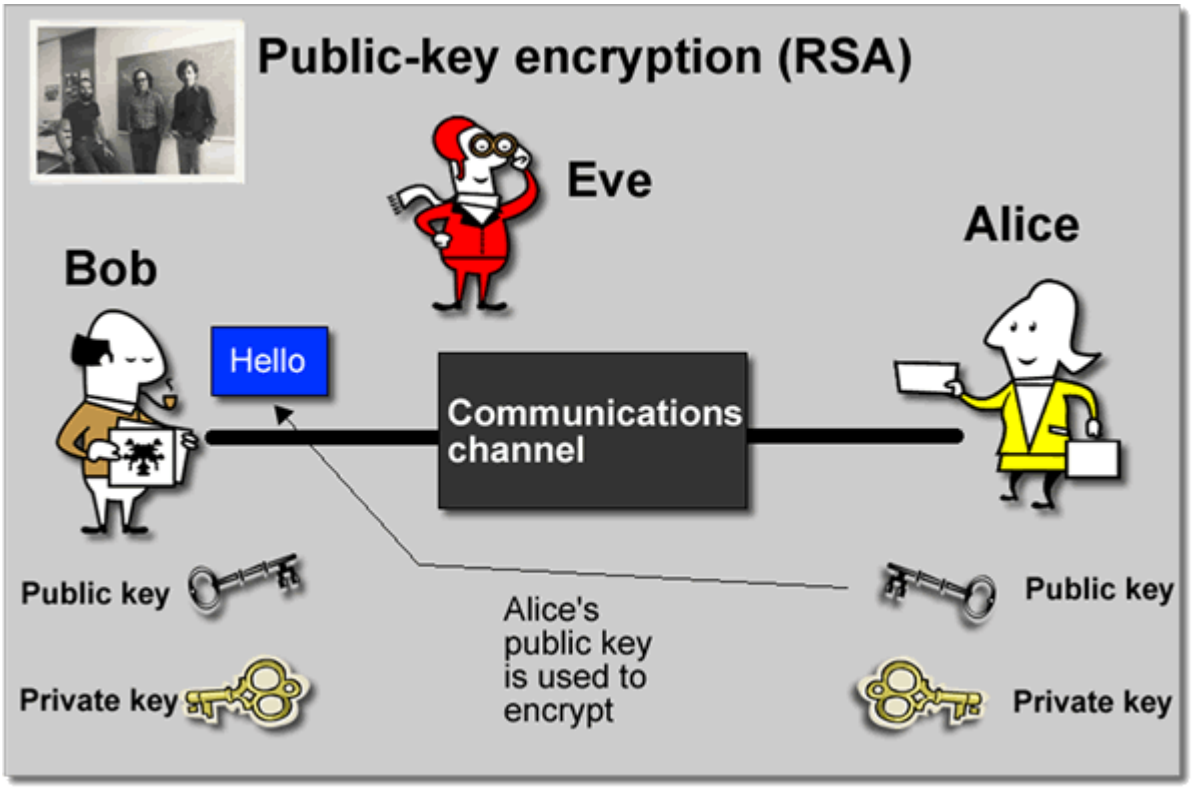
١. لە دی ئی ئێس DESدەچێت: سایفەریی قاڵبە Block Cipher لەگەڵ شێوەی جیاواز، بەڵام قاڵبەکانی ١٢٨ بتە 128 Bit Blocks.
٢. کلیلی ١٢٨ بتی ، 192 بتی یان ٢٥٦ بتی هەیە.
٣. ئالوگۆڕێکی تێکەڵی هەیە، سنووقەکانی ئیس S- Boxes.
٤. سنووقەکانی ئیس S – Boxes لەسەر بنەمایی حسابکردنی پۆلینۆمییەڵە Polynomial، ئەمەش هیڵی نی یە Non – Linear و، ئاسانە بۆ شیکردنەوە.



ئار ئیس ئەی

RSA

ئار ئیس ئەی RSA: ئەم ئەلگۆریسمە (ئار ئیس ئەی RSA) کورتکراوەی Rivest Shamir Adleman ـە و، لەلایەن رۆن ریڤێست Ron Rivest، ئادی شامیر Adi Shamir و لێن ئادلیمانەوە Len Adleman دروستکرا و، ناوەکەی لە یەکپێگرتنی ناوی هەرسێکیان پێکهاتووە، لە ساڵی ١٩٧٨، ئەلگۆریسمی کلیلی گشتی Public Key یە، ئەم ئەلگۆریسمە بەکاردێت بۆ بەهێما کردن Encryption و ئیمزا لە سەر زانیاری Data Signing، کرداری بە هێماکردن Encryption و، ئیمزا لە سەر زانیاری Data Signing بە ئەنجام دەگات لە رێگەی زنجیرەیەك لێکدانەوە.



بەشی پێنجەم

کریپتۆ گرافی و ئیف ئیس

لە مایکرۆسۆفت ویندۆز دا

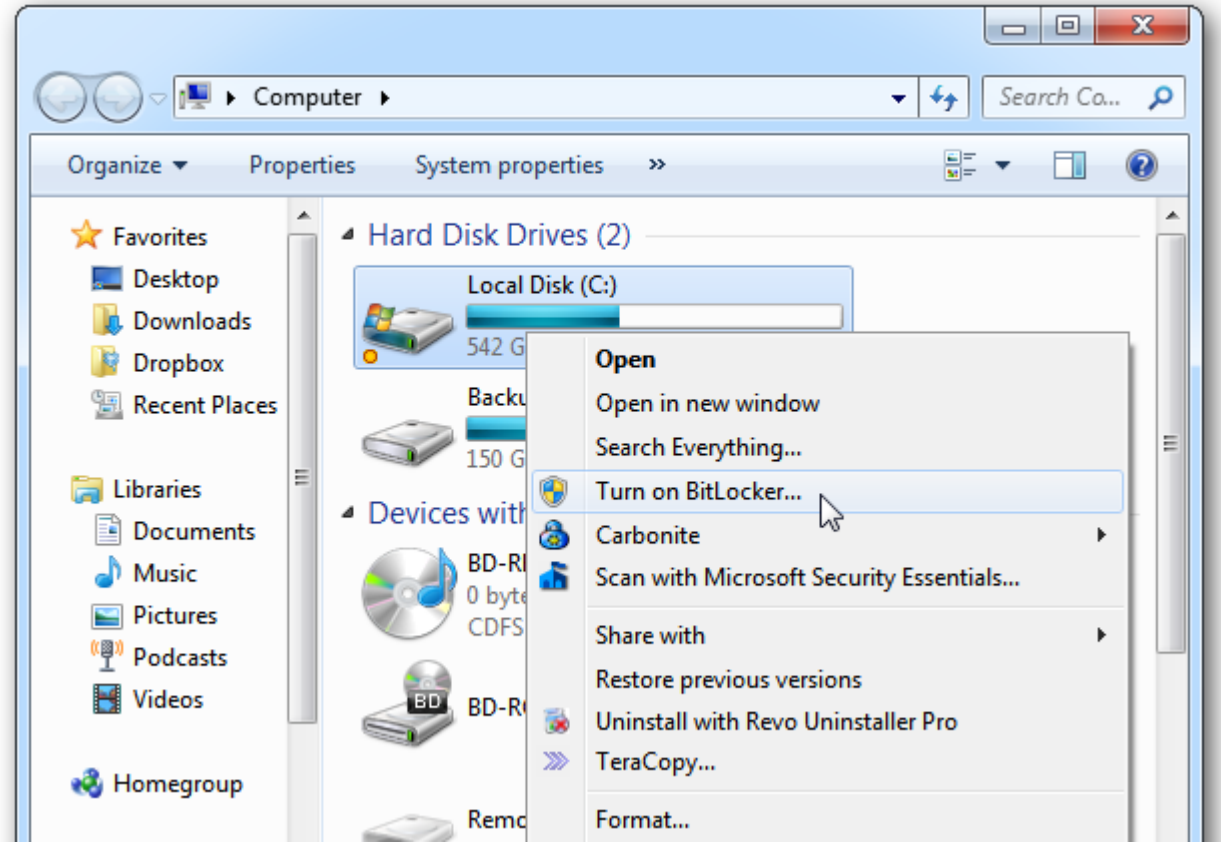
بـــــتـــــلـــــۆکـــــەر

Bit Locker

بتلۆکەر Bit Locker بەهێماکردنی تەواوی بەشەکانی کۆگایە Full Disk Encryption کە لە نەوەی مایکرۆسۆفت ویندۆز دا هەیە، ئەمەش دابینکراوە بۆ پاراستنی زانیاری ئەمەش لە رێگەی بە هێماکردنەوە Encryption. بە شێوەیەکی هەمیشەیی ئەلگۆریسمی ئەی ئی ئێس AES Algorithm بەکاردەهێنێت لەگەڵ ١٢٨بت یان ٢٥٦ بت لە کلیل Key، هەروەها سوود لە تەکنیك و شێوەی تریش وەرگیراوە بۆ بەهێزکردنی پاراستنەکە، وەکو : Elephant Diffuser.

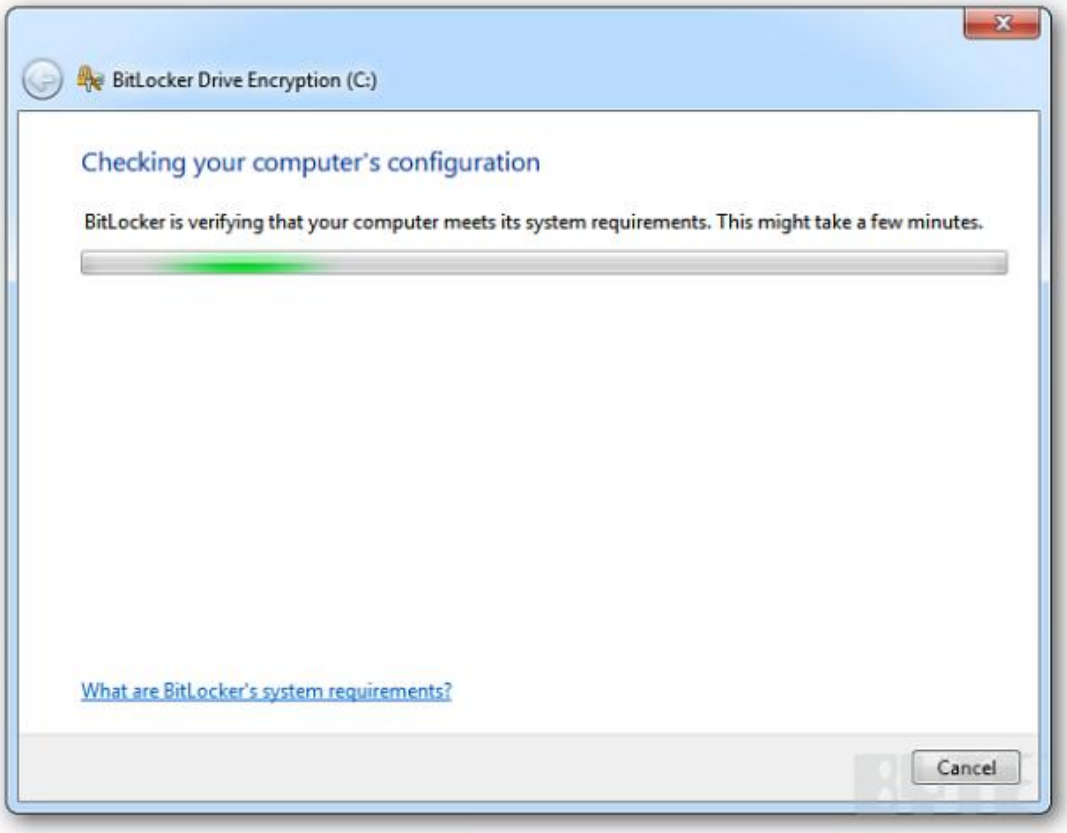
بۆ بەکارهێنانی بتلۆکەر لە ویندۆزی حەوت دا، ئەم هەنگاوانە جیبەجێدەکەین:

١. بەشی کۆمپیوتەر Computer بکەرەوە.
٢. کلیلکی راست لەسەر بەشی سی :Local C بکە.
٣. کلیك لەسەر کاپێکردنی بتلۆکەر Turn On Bitlocker بکە.

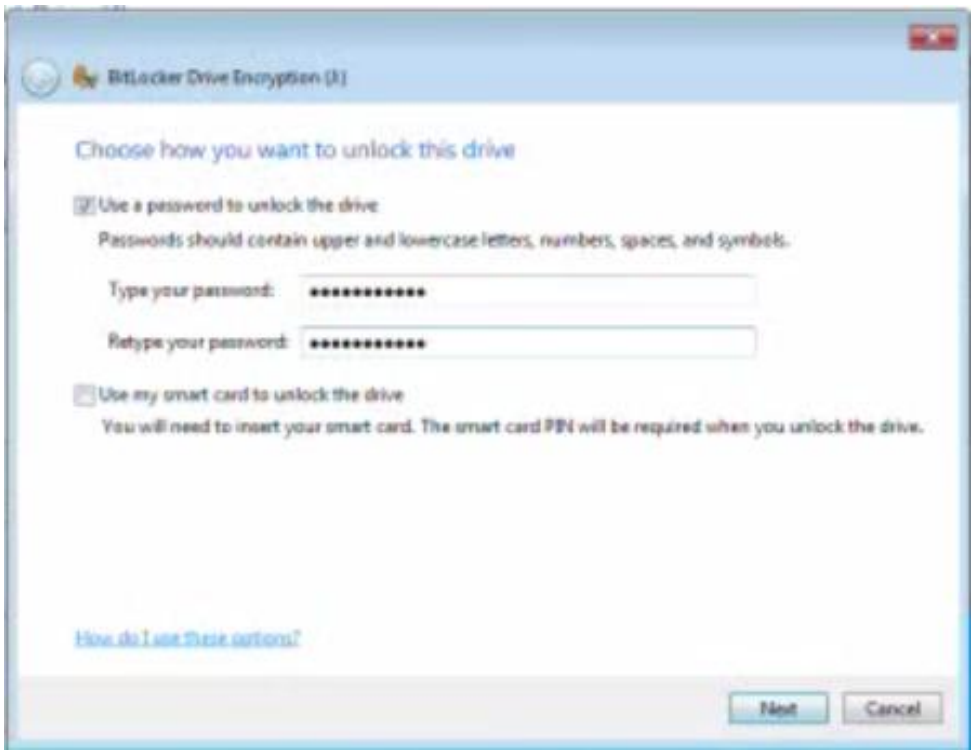


٤. پاشان بتلۆکەر Bitlocker دەست دەکات بە پشکنینی سیستەمەکەت، بۆ دڵنیابوونەوە لەوەی

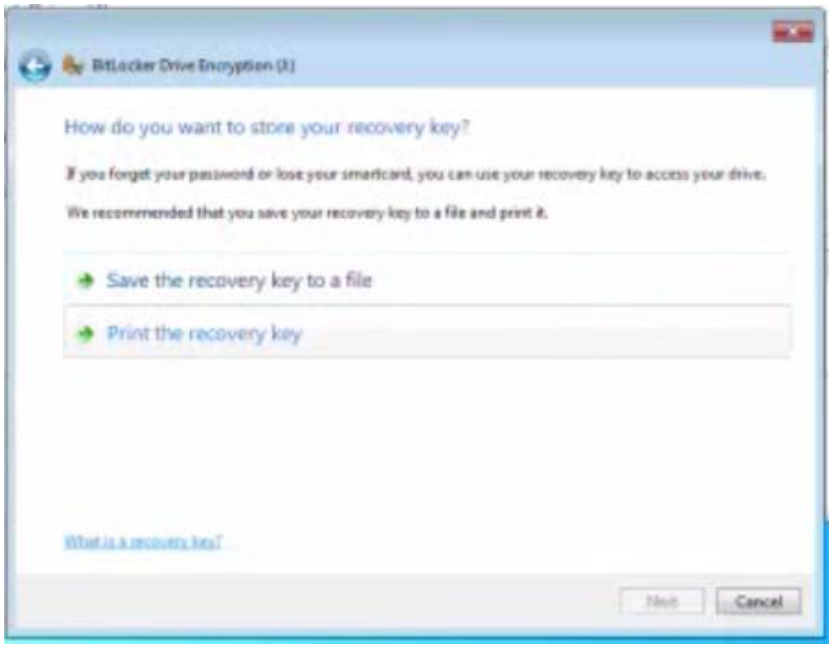
هەنگاوەکانی دابەزاندن رووی داوە:



٥. پاشان کلیك لەسەر Use Passwordبکە و تیپەڕەوشە Passwordدابنێ:



٦. کاتێك سێهەمت هەلبژارد واتە داواکراوبێت لەکاتی هەموو کارپێکردنێکدا، پاشان شوێك دیاری بکە بۆ پاشەکەوت Save کردنی کلیلی گەراندنەوە و، وا پێویستە لە هەمان شوێن خەزنی نەکەیت.



٧. پاشان کلیك لەسەر دەستکردن بە بەهێماکردن Start Encryption بکە.

٨. هەندێك کاتی دەوێت و پاشان کارەکە بە ئەنجام دەگات.

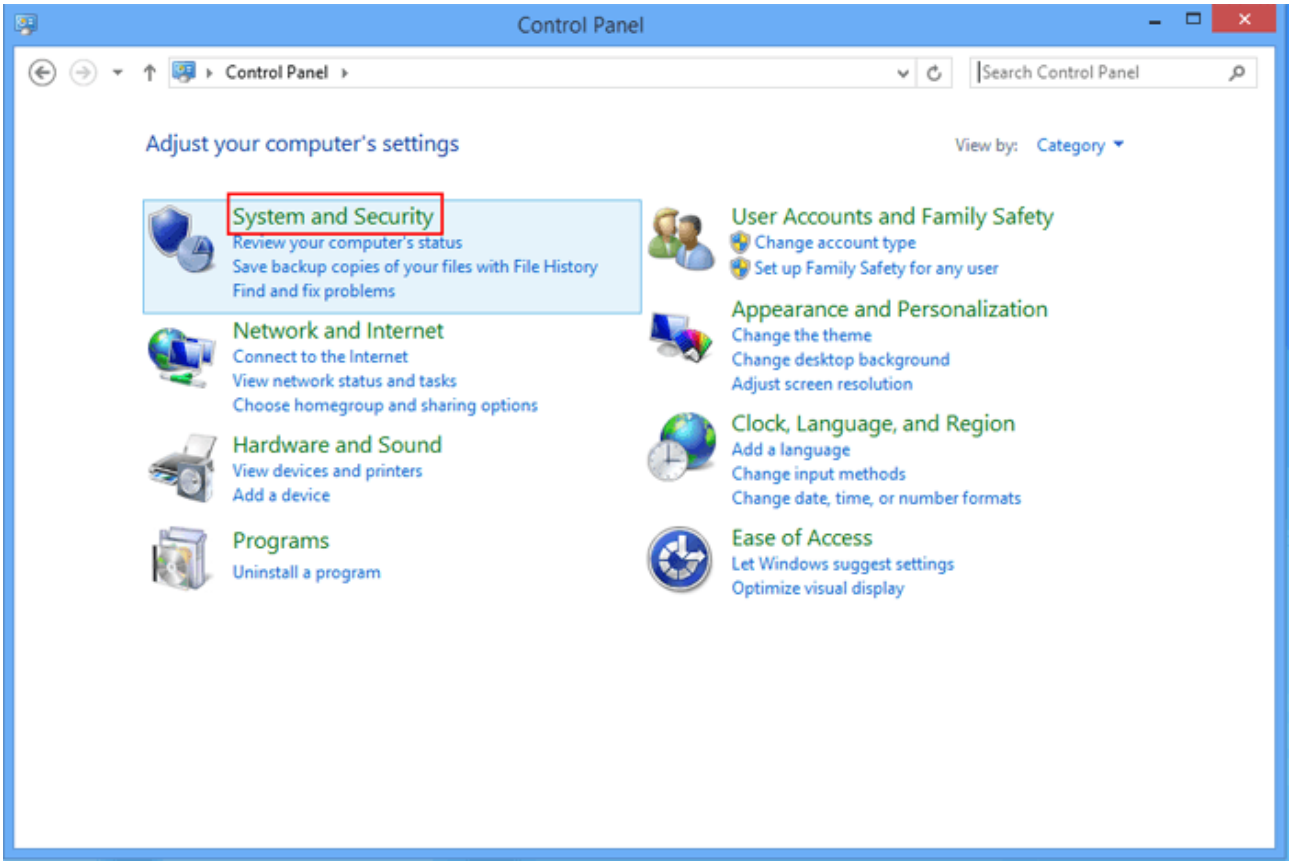
٩. بەمەش کارەکە بە کۆتا گەیشت و، بۆ کردنەوەی داوای تیپەرە وشەدەکات و، پاشان دەیگیرێتە بۆ شێوەی ئاسایی Decrypt.

بتلۆکەر لە ویندۆزی هەشت دا

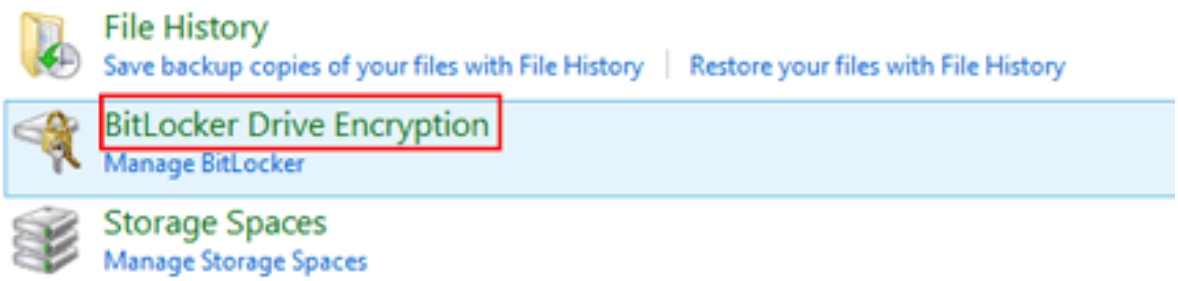
Bitlocker in Windows 8

١. بەشی دەست بەسەراگرتن Control Panel بکەرەوە.

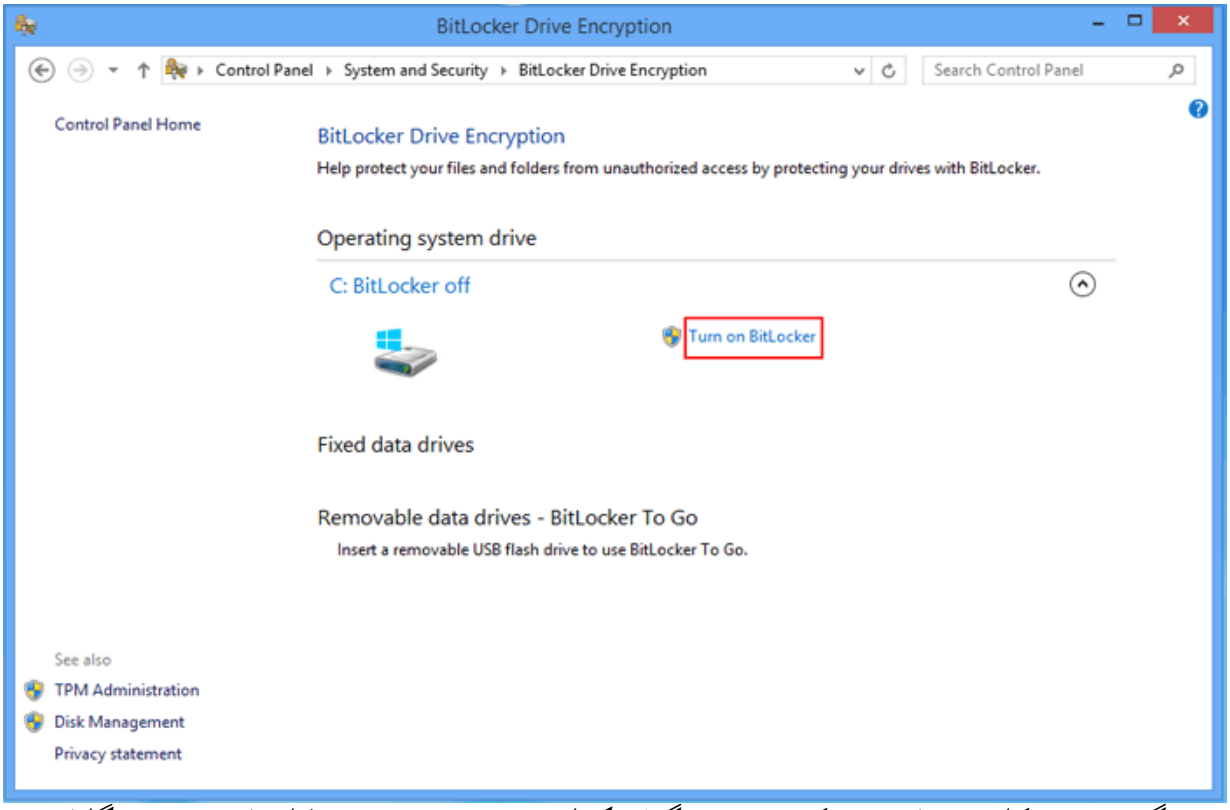
٢. بەشی System & Security بکەرەوە.



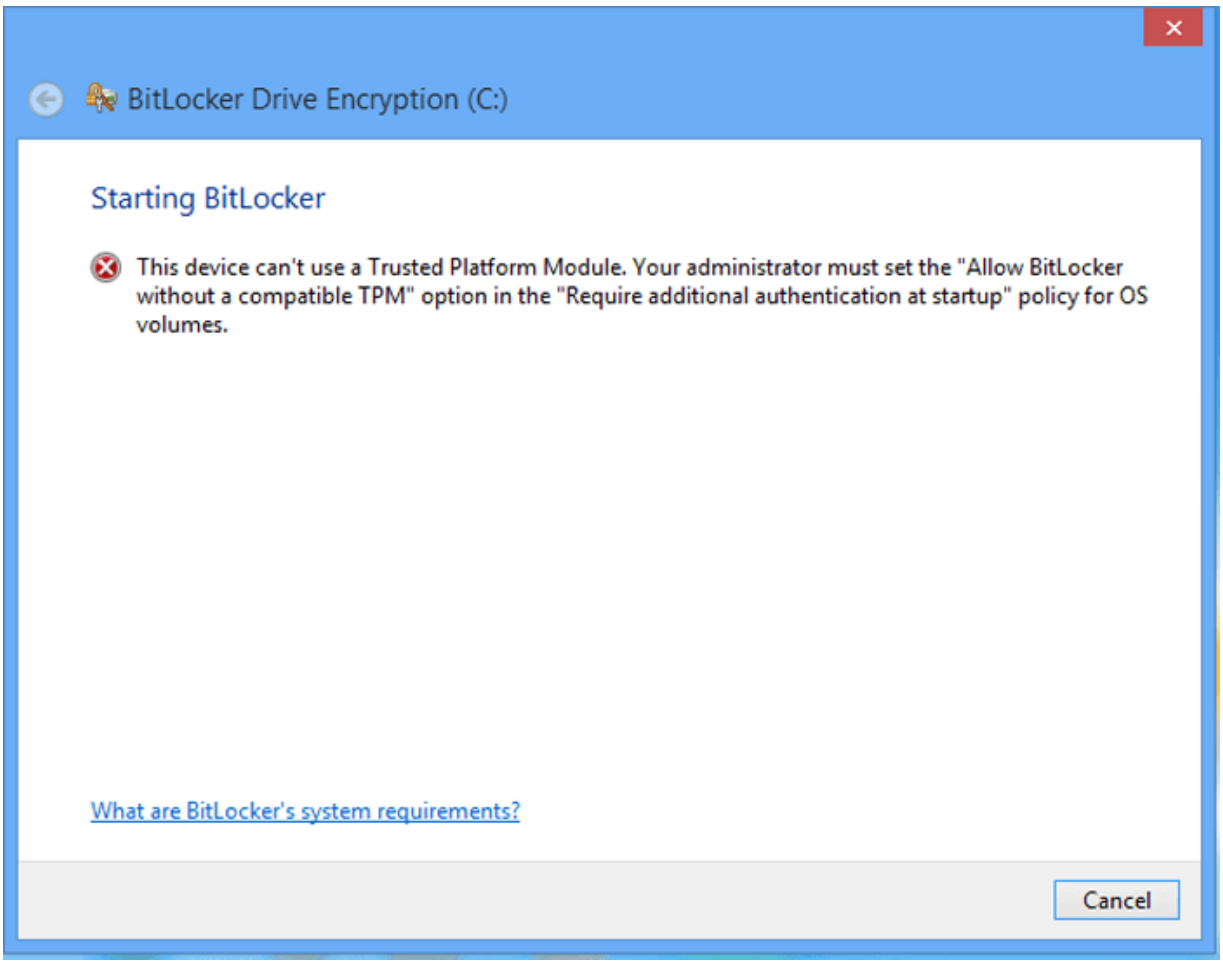
٣. بەشی Bitlocker Drive Encryption بکەرەوە.



٤. کلیك لەسەر کارپێکردنی بتلۆکەر بکە Turn On Bitlocker.

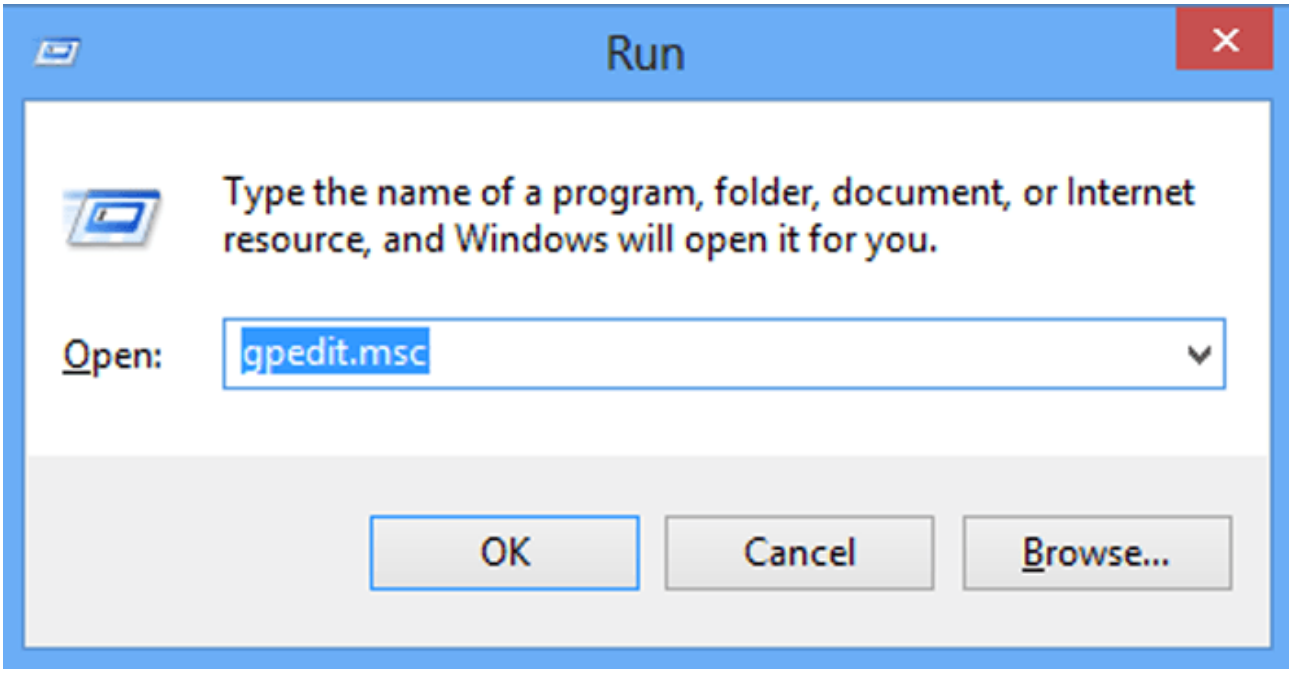


٥. ئەگەر ئەم رووکارەی خوارەوە دەرکەوت، ئەوە گرفتێکمان هەیە و دەبێت بە ئەنجامدانی ئەم هەنگاوانەی خوارەوە چارەسەری بکەین و، پاشان بگەڕێینەوە سەر تەواو کردنی کارەکەمان:

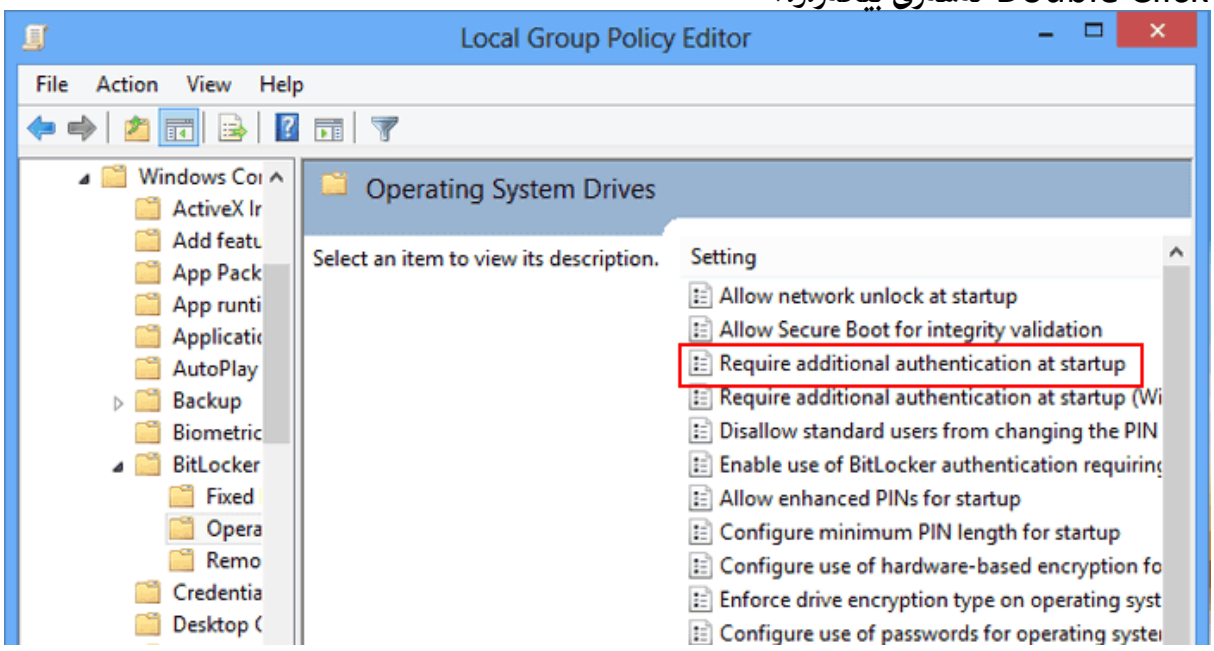


یەکەم// پەنجەبنێ بە دوگمەی پەنجەرەو پیتی ئار Widows Key + R بۆ کردنەوەی پەنجەی جیبەجێکردن .Run

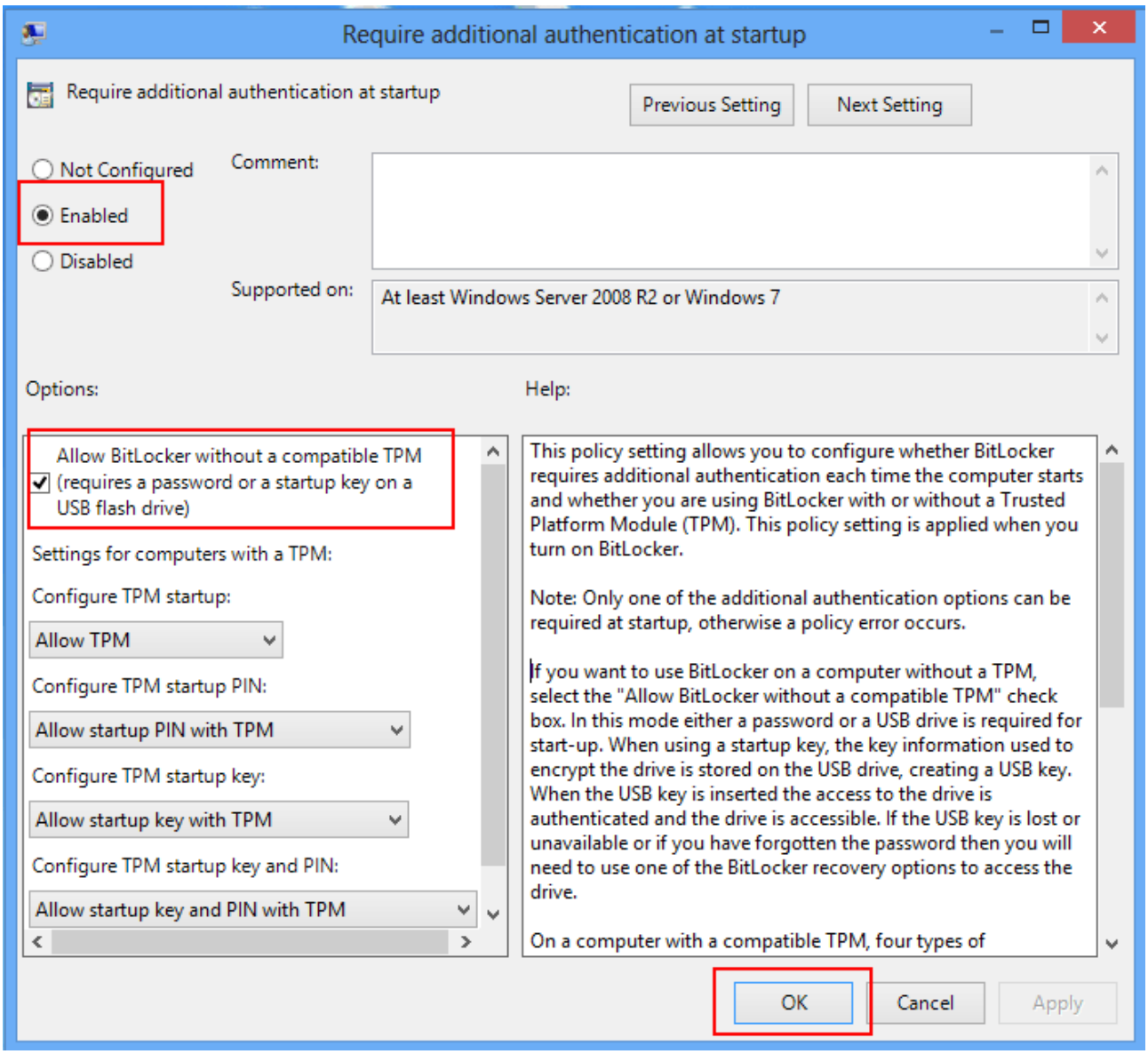
دووەم// لە خانەی تایبەت بە کردنەوە Open ی پەنجەرەکەی کرایەوە بنووسە gpedit.msc و کلیك لەسەر دووگمەی Ok بکە:



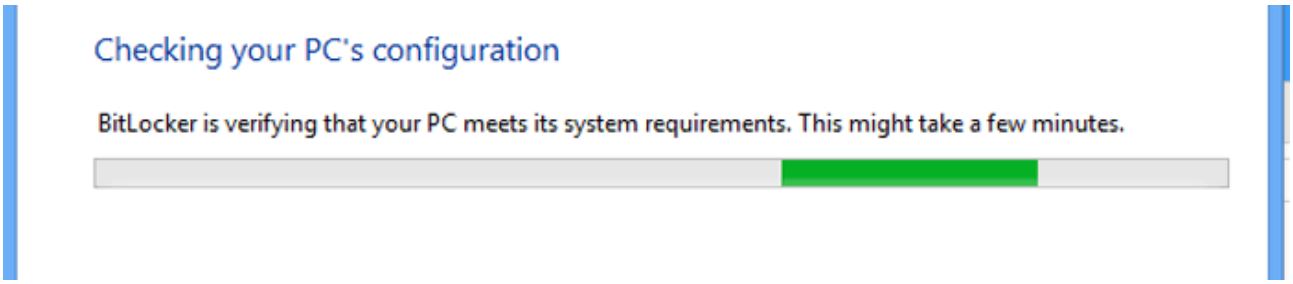
سێهەم// بگەڕێ و Require Additional authentication at startup بدۆزەرەوە و، بە دووانە کلیك Double Click لەسەری بیکەرەوە:



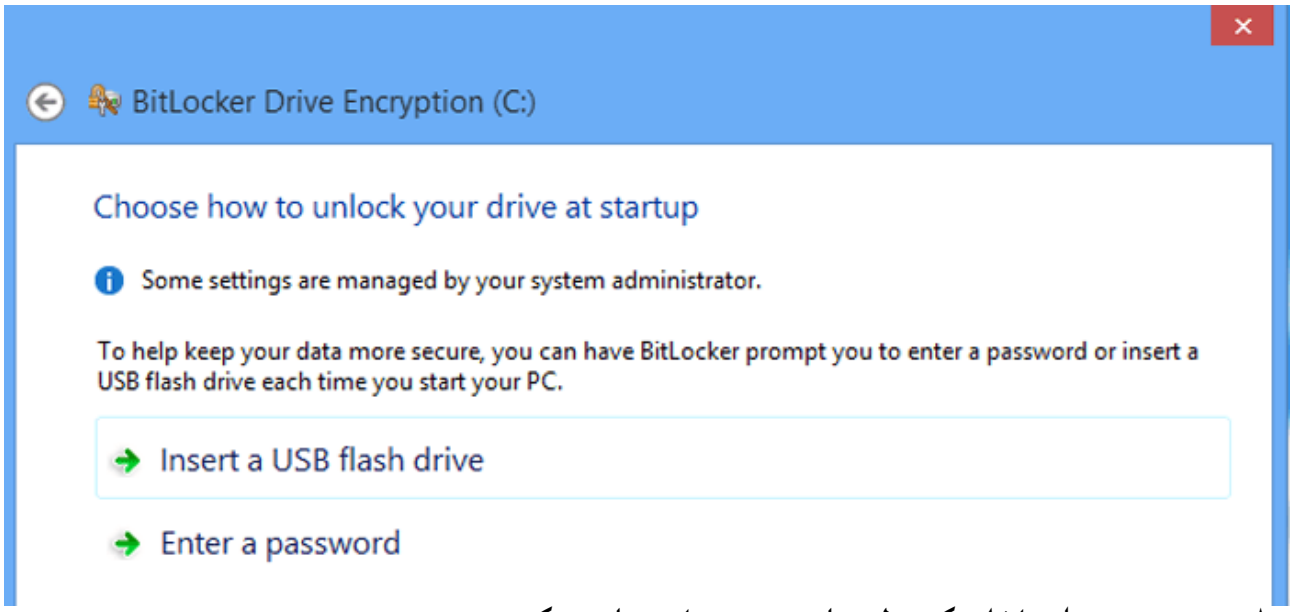
چوارەم// کلیك لەسەر Enable بکە و، پاشان کلیك لەسەر ..... Allow Bitlockerبکە و، لە کۆتایدا کلیك لەسەر Okبکە.



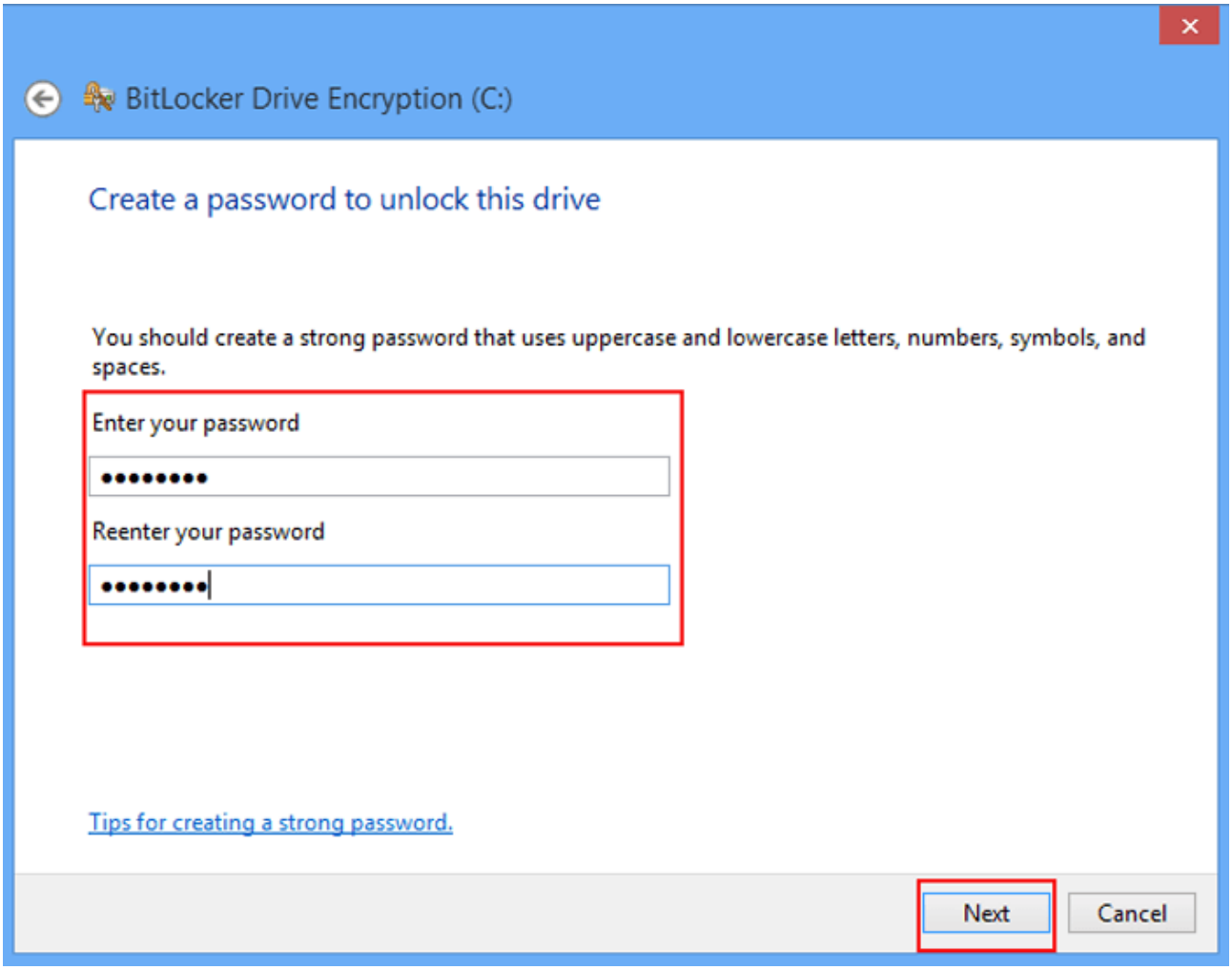
٦. ئیستا جاریکی تر کلیك لەسەر کارپێکردنی بتلۆکەر Turn On Bitlocker دەکەینەوە، و کەمیك چاوەروان دەبین.



۷. ئەم رووکارەی خوارەوە دەکریتەوە و کلیك لەسەر داغلّکردنی تیپەرە وشە Enter Password بکە.

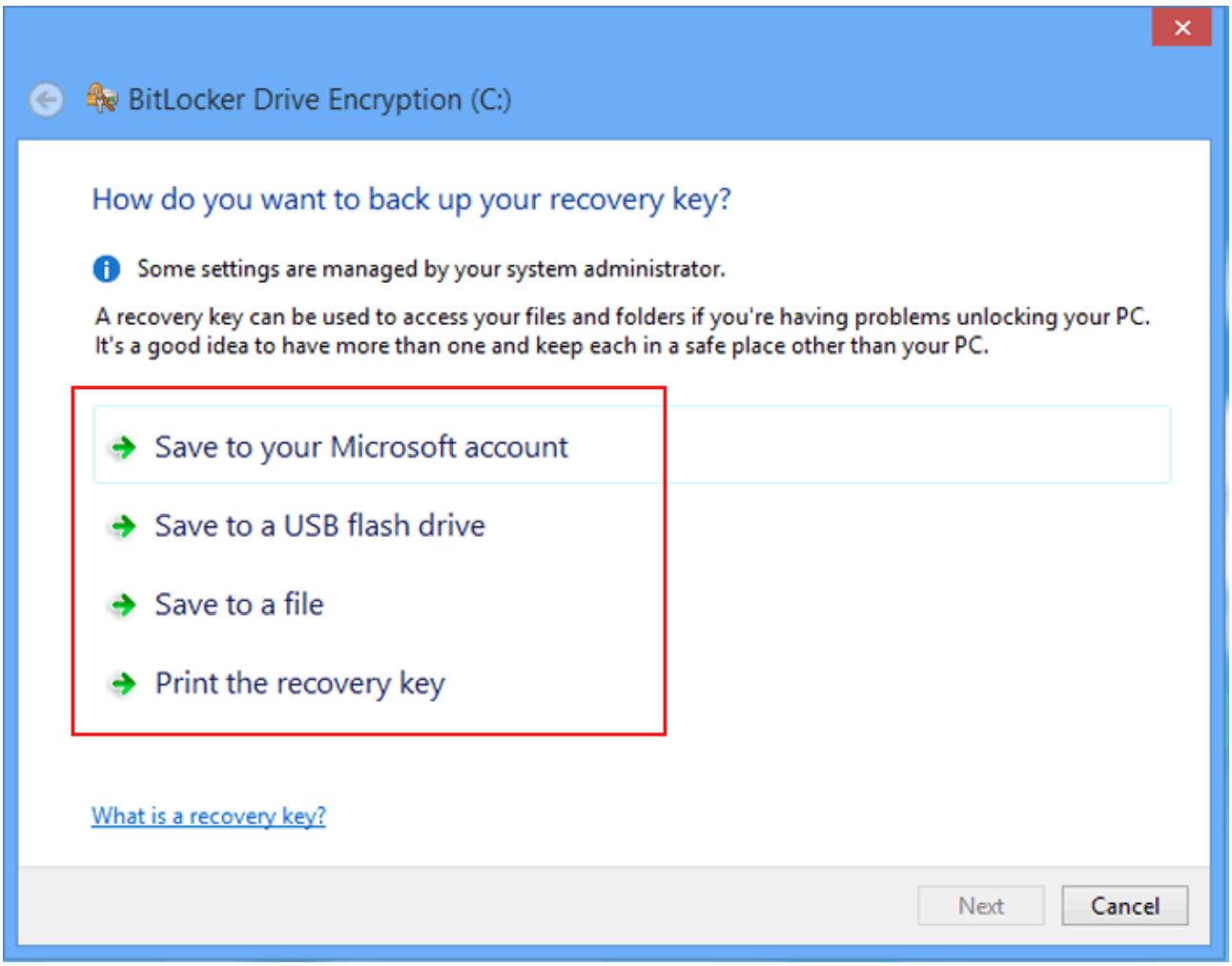


۸. تیپەرە وشەیەك داغلّ بکە و لە خانەی دووەم دا دووبارەی بکەرەوە.



۹. کلیك لەسەر Next بکە.

١٠.یەکیك لە دراوەکان هەلبژێرە بە گوێرەی پێویستی و ویستی خۆت:



١١.پاشان کەمێك چاوەری بکە و، کلیك لەسەر Next بکە.

١٢.یەکێك لەو دوو شێوەیە هەلبژێرە و کلیك لەسەر Next بکە.

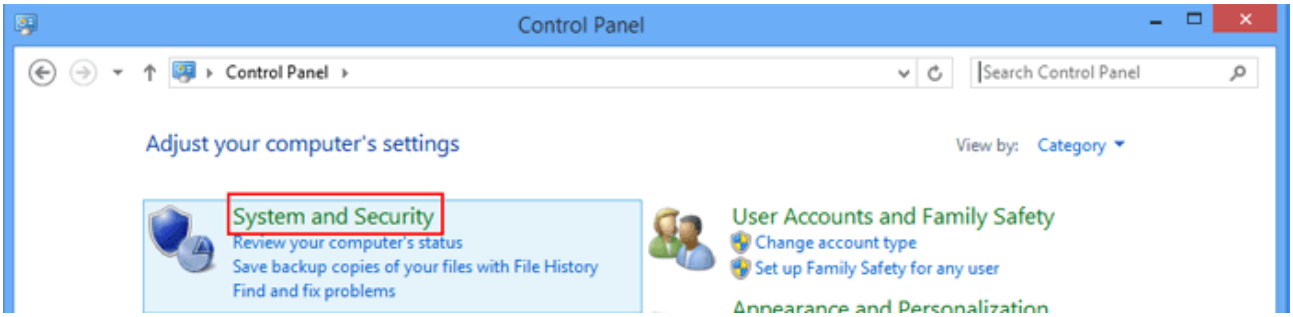
١٣.بەردەوامبە و کلیك لەسەر Restart بکە .

گۆرین و لابردنی تیپەرە وشەی بتلۆکەر

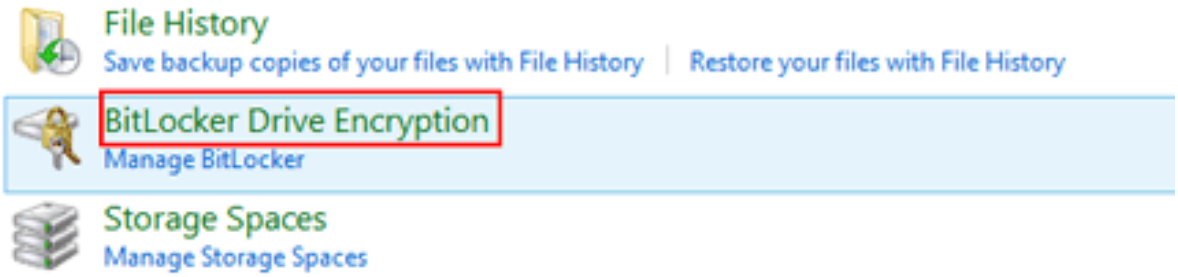
Change and Remove of Bitlocker Password

١. بەشی دەست بەسەراگرتن Control Panel بکەرەوە.

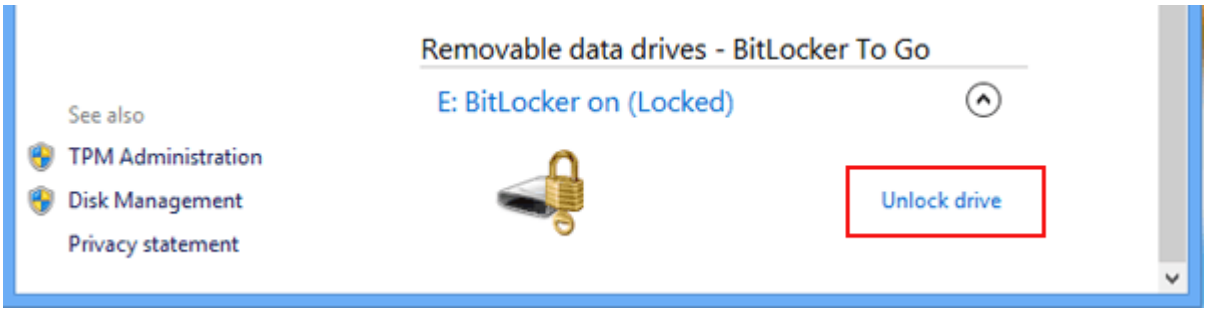
٢. بەشی System & Security بکەرەوە.



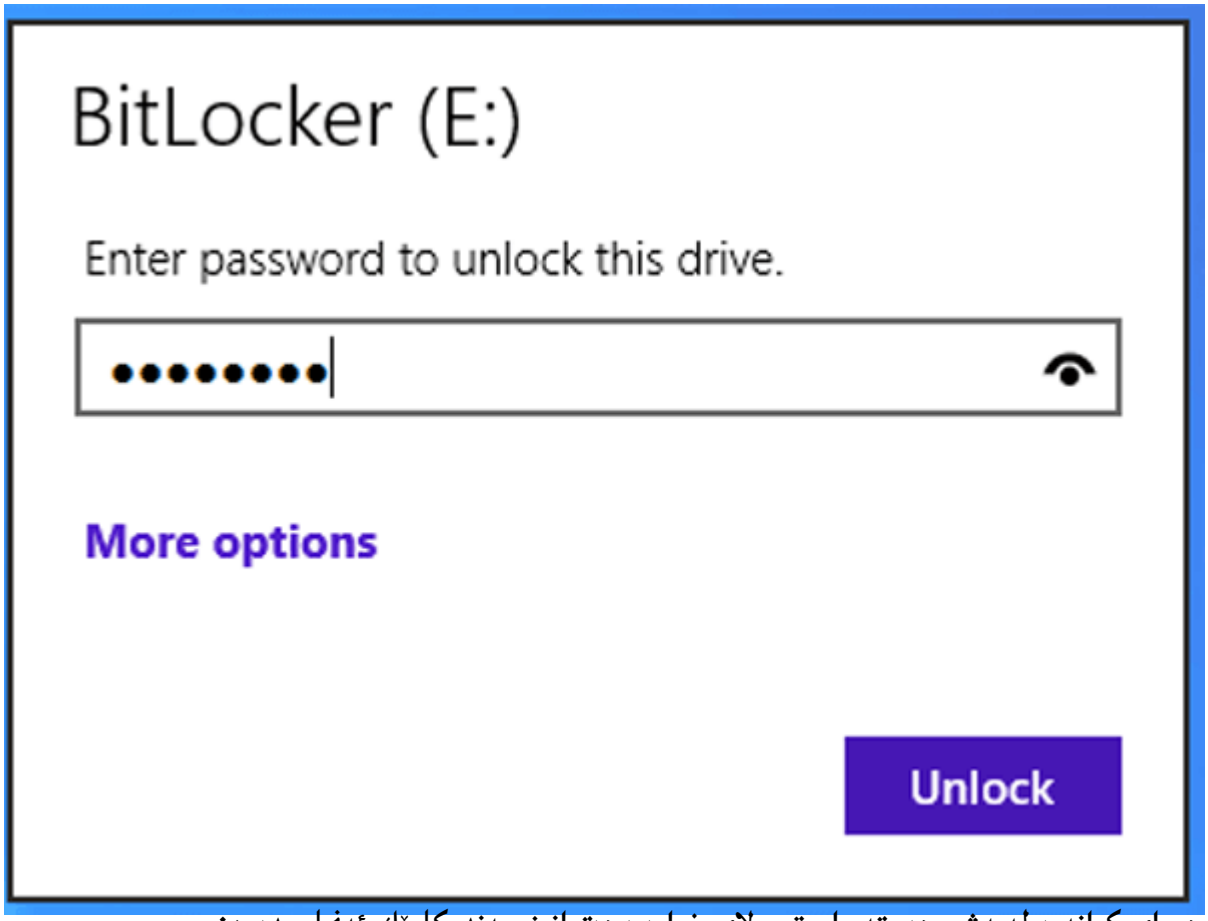
٣. بەشی Bitlocker Drive Encryption بکەرەوە.



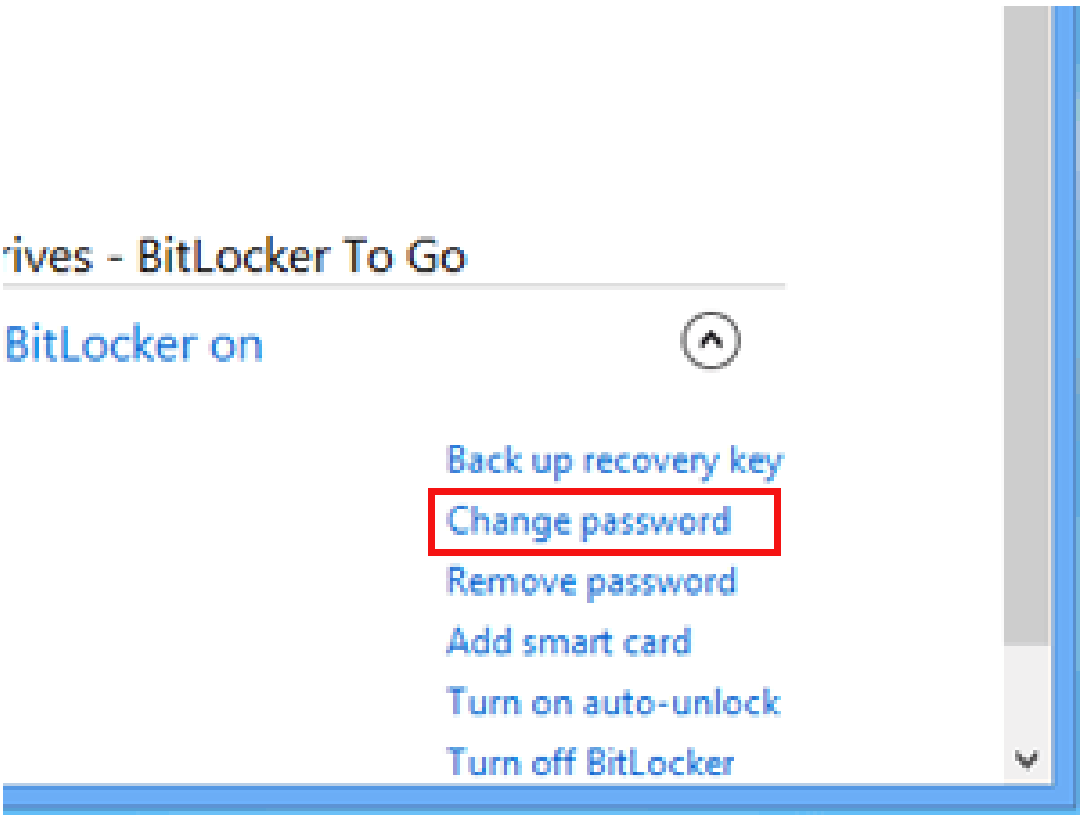
٤. کلیك لەسەر کردنەوەی بتلۆکەر Unlock Drive بکە:



٥. تیپەرە وشەکەت Password داغڵبکە و، کلیك لەسەر Unlock بکە.



٦. دووای کرانەوە لەبەشی دەستە راست و لای خوارەوە دەتوانین چەند کارێك ئەنجام بدەین:



- نووسخەی یەدەگی کلیلی گەراندنەوە Back Up Recovery Key.
- گۆرینی تێپەرە وشە Change Password.
- لابردنی تیپەرە وشە Remove Password.
- زیاد کردنی کارتی زیرك Add Smart Card.
- کارپێکردنی کردنەوەی خودکار Turn On Auto-Unlock
- کوژاندنەوەی بتلۆکەر و لەکار خستنی Turn Off Bitlocker.

تەشفیری فایل و فولّدەرەکان بەبەکارهێنانی سیستەمی فایل تەشفیر کردن (ئی ئێف ئێس)

Encrypt Files and folders using Encrypting File System (EFS)

سیستەمی فایل تەشفیرکردن چییە؟

What is Encrypting File System (EFS?)

ئی ئێف ئێس هەڵدەستێت بە دابینکردنی تەکنەلۆژیایی تەشفیرکردنی ناوکی فایل و، بەکاردێت بۆ خەزنکردنی فایلە تەشفیرەکان لەسەر سیستەم فایلی ئین تی ئیف ئێس NTFS File System. هیچ کەسێك ناتوانێت دەستی بگات بەو فایل و فولّدەرانەی کە تەشفیر کراون، تەنها بەکارهێنەر نەبێت کە فایل و فولّدەرەکەی تەشفیر کردووە.

تەشفیرکردنی فایل و فولّدەر

Encrypt File or Folder

١. ئەو فایل یان فولّدەرە دیاری بکە و هەلیبژێرە Select کە دەتەوێت تەشفیری Encrypt بکەیت.
٢. کلیکی ڕاست Right Click ی لەسەر بکە، پاشان کلیك لەسەر تایبەتمەندییەکان Properties بکە.
٣. لە تابی گشتی Generalدا، کلیك لەسەر پێشکەوتوو Advanced بکە.
٤. کلیك لە سندوقی پشکنین Check Box ی بەردەم Encrypt Contents to Secure Data بکە.
٥. دەبینیت فایل یان فولّدەرەکە تەشفیربوو، ڕەنگی ناوەکی گۆڕا بە سەوز.

دەستگەیشتن بە فایل و فولّدەری تەشفیر لەلایەن دوو بەکارهێنەرەوە

Access an Encrypted File or Folder by 2 Users

١. دوو حساب دروستە دەکەین لە کۆمپیوتەرەکەماندا، بە جیبەجێکردنی ئەم هەنگاوانی لای خوارەوە:

- کلیکی ڕاست لەسەر Computer دەکەین لەسەر ڕووی شاشەکە.
- کلیك لەسەر Manage دەکەین.
- کلیك لەسەر Local User and Groupدەکەین، پاشان کلیکی ڕاست لەسەر User دەکەین.
- کلیك لەسەر New Userدەکەین و، پاشان ناوی بەکارهێنەر User Name و، تیپەڕە وشە Password دەنووسین.
- لەخانەی Confirm Passwordدا، دووبارە تیپەڕە وشەکە Password دەنووسینەوە.
- دروستە کردن Create.

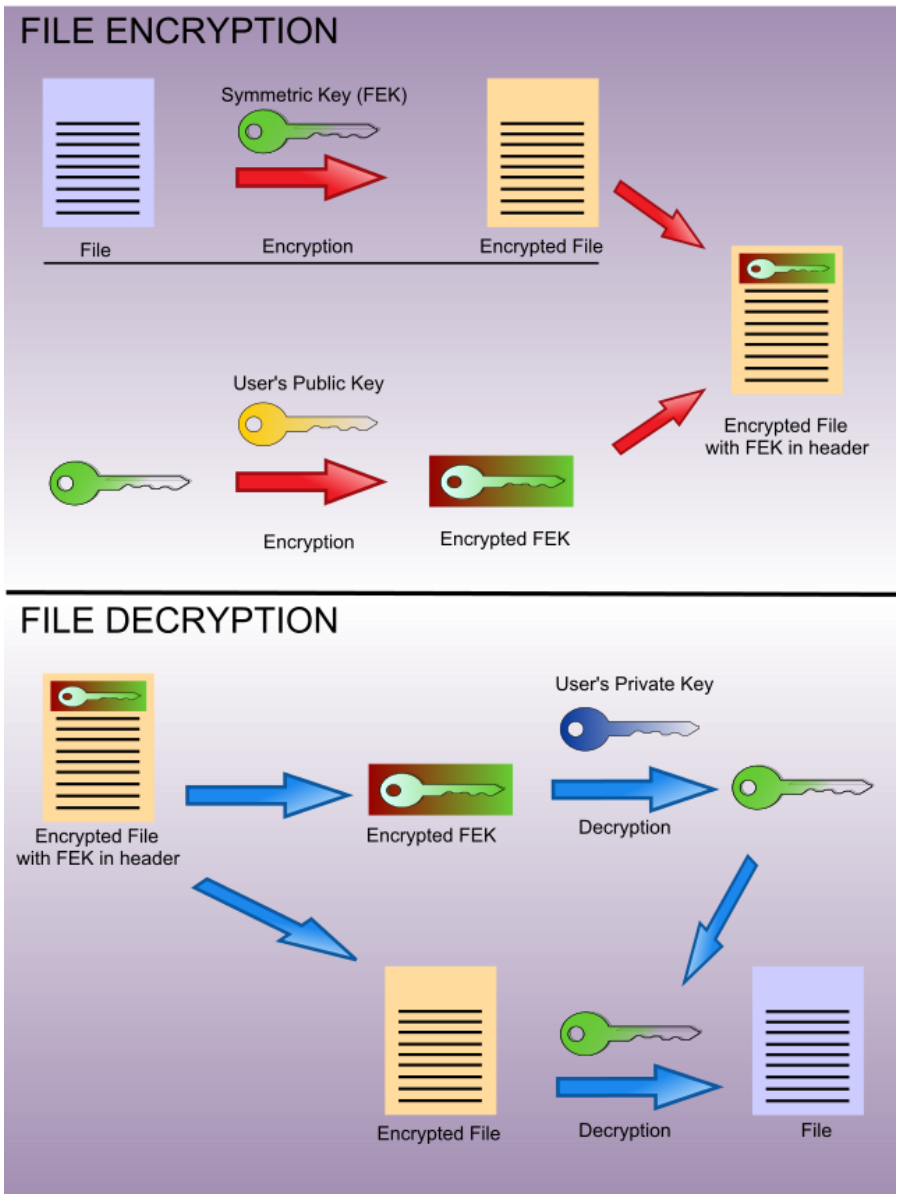
بەهەمان ڕێگەی سەرەوە حسابی بەکارهێنەری دووەمیش Second User Account دروستت دەکەین.

پاشان بە حسابی بەکارهێنەری یەکەم First User Accountداخڵ دەبین:

Ctrl + Alt + Del لێبدە و، پاشان ناوی بەکارهێنەر User Name و، تیپەڕە وشە Password بنووسە و، داخڵ ببە.

فایلێك File یان فۆلدەرێك Folderتەشفیر Encrypt بکە.

ئیستا لۆگ ئۆف Log off بکە و، بە حسابی بەکارهێنەری دووەم داخڵ ببەرەوە و، هەوڵبدە فایلە تەشفیرەکە بکەیتەوە، سەیر دەکەیت ناتوانی ئەو کارە بکەیت و، ڕێگەت پێنادات و، قبووڵی ناکات.



بەشی شەشەم

ستیگانۆگرافی و

ۆتەرمارکینگ

ستیگانۆ گرافی

Steganography

هونەر و زانستیکە بۆ شاردنەوەی نامە و پەیامێکی شاراوە Hidden Message، بەدانانی نامە و پەیامەکە لەناو هی تردا، بە هۆی چەند ڕێگایەکەوە.پەیامەکە بە ڕووالّەت وادەردەکەوێت کە ئاساییە و بێزیانە.

شاردنەوە Steganography کاردەکات بە لە جیاتی دانانی بتە زیادەکانی زانیارییەکە یان بتە بەکارنەهاتووەکان لە ناو فایلەکانی کۆمپیوتەردا، وەکو ((گرافیکەکان Graphics، نووسین Text ، هتملّ HTML، ڤیدیۆ Video، دەنگ Sound و یان .....)) لەگەلّ بتە جیاوازەکان، ئەم شاردنەوەی زانیارییە دەتوانرێت : نووسینی ئاسایی Plain Text، سایفەر Cipher، و وێنەکان بێت.

وشەی ستیگانۆ گرافی steganography لە دووبەش پێکهاتووە و، لە وشەی ستیگانۆ Steganos ی یۆنانی کەبەمانای داپۆشەر Covered دێت، لەگەلّ وشەی گرافی Graphy کە بەمانای نووسین Writing یان کێشان و هێلّکاری Drawingدێت، وەرگیراوە.

کەواتە دەتوانین ستیگانۆ گرافی Steganography بەوە پێناسە بکەین کە پرۆسەی Process شاردنەوەی نامە و پەیامی نهێنییە Secrete Message، وە هەروەها دەرهێنانەوە و وەرگتنەوەی نامەکە لە لایەن وەرگرەوە Destination.

هەرکەسێك نامە و پەیامە ڕوون و ئاشکراکە ببینێت، نازانێت کە نامە و پەیام و داتای نهێنی Encrypted Data تیایە، واتە بەشتە شاراوە Hidden و بەکۆدکراوەکان Encrypted Data نازانێت کە تیایەتی.

ستیگانۆ گرافی و کریپتۆگرافی

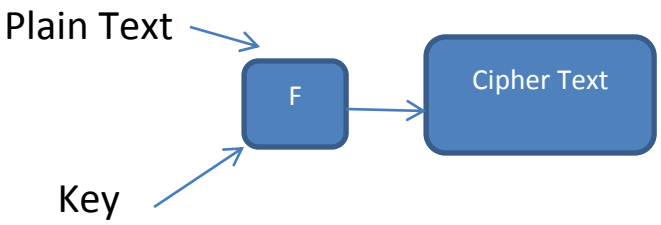
Steganography & Cryptography

لە راستی دا بەکۆد کردن و گۆڕینی زانیارییە روون و دیارەکان بۆ زانیاری نا روون و نهێنی Encryption **بەس نییە و، هەموو شتێك نییە، بۆیە لە گرفت و کێشەی سجنەوە جۆر و ڕێگەی دیکەش دروووست بوو. دوو سجن ((بەند کراو)) پلانی ڕاکردنیان هەبوو، بەلام هەموو ڕێگەکانی پەیوەندی کردن، لە ڕێگەی چاودێر و پاسەوانێکەوە بوو، کە هەموو نامە و پەیامە شاراوە و نهێنییەکانی** Encrypted Message **کەشف دەکرد و دەیدۆزییەوە، هەروەها بە ئاسانی دەیتوانی هۆیەکانی گەیاندن و پەیوەندی بوەستێنێت، بۆیە پێویست بوو ئەم دوو گیراوە ڕێگەیەك بدۆزنەوە بۆ شاردنەوەی نامە و پەیامە نهێنییە گرنگەکان** Secret Message**، بەم هۆیەوە ستیگانۆ گرافی دروووست بوو. ستیگانۆ گرافی و کریپتۆگرافی لە راستی دا ئامۆزای** Cousin **یەکترن، لەکاتێکدا ئامانجی سیستەمی کریپتۆگرافی شاردنەوەی ناوەرۆکی نامەکانە، بەلام ئامانجی شاردنەوەی زانیاری** Information Hiding **یان ستیگانۆ گرافی شاردنەوەی ئەوەیە کە هەیە.**

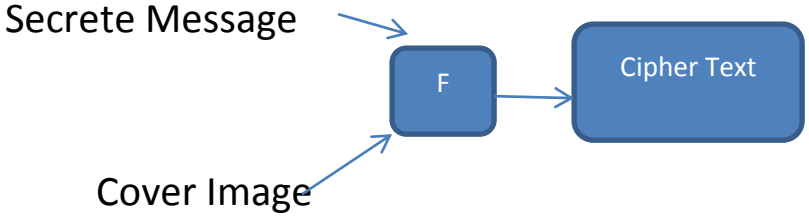
کریپتۆگرافی Cryptography

$C=E_k(P)$

$P=D_k(C)$



ستیگانۆگرافی Steganography



ستیگانۆگرافی نوێ

Modern Steganography

ستیگانۆگرافی تازە دەگەڕێتەوە بۆ شاردنەوەی زانیاری لەناو وێنەی دیجیتالی یان دەنگ دا، کاردەکات بە لە جیاتی دانانی بتەکانی زانیاری بەکارنەهاتوو لە فایل دا، لەگەڵ بتەکانی زانیاری پیشان نەدراو.

پێویستی و داواکارییەکان

Requires

بۆمەبەستی خستنە ناو شاردنەوەی زانیاری بۆ ناو وێنە دوو فایل پێویستە، فایلی وێنەی داپۆشەر The Cover Image **کە زانیارییە شاراوەکە هەڵدەگرێت** Hold the hidden Data **، هەروەها فایلی نامەی نهێنی** Secret Message File.

نامە Message **لەوانەیە نووسینێکی ئاسایی بێت** Plain Text**، یان نووسینی بە کۆد کراو** Cipher Text**، یان وێنەیەکی تر، کاتێك هەردووکیان دەکرێن بەیەك** Combine **واتە** Cover Image **و** Hidden (Secrete) Message **ئەوا ستیگۆ ئیمەیج** Stego Image **دروست دەبێت. هەروەها ستیگۆ کی** Stego Key **یان تێپەڕە وشە** Password **لەوانەیە بەکاربهێنرێت بۆ شاردنەوە** Hide **و کردنەوەی کۆد** Decode **نامەکە.**

- **وێنەی داپۆشین** Cover Image: **وینەیەکە، کە بەکاردێت بۆ شاردنەوەی** Hide **نامە و پەیامێکی پەنهان ((نهێنی))** Secret Message.
- **نامە ((پەیام/ ڕاسپاردە)) ی نهێنی ((پەنهان))** Secret Message: **نامە و پەیامێکی نهێنی و گرنگە، کە دەمانەوێت بیشارینەوە** Hide **و بیپارێزین لەوەی دەست کەسانێك بکەوێت کە دەبنە مایەی مەترسی و هەڕەشە بە دەست کەوتنی ئەو زانیارییانە.**
- **وێنەی ستیگۆ** Stego Image: **یەکخستن و تێکەڵاوکردنی** Combine **وێنەی داپۆشین**

Cover Image و، نامەی نهێنی و پەنهان Secret Message یان نامەی شاراوە Hidden Message ، ئەم وێنەی ستیگۆیە بە هۆی کلیك Key و دوو بەشەوە دروستدەبێت.

- تێپەڕە وشە Password یان کلیلی ستیگۆ Stego – Key: لەوانەیە بەکاربهێنرێت بۆ شاردنەوە Hide و ئاسایی کردنەوە و پیشاندانەوەی نامەکە Decode Message.

پرۆسەی ستیگانۆ گرافی

Steganography Process

ئەو زانیارییەی دەمانەوێت بیشارینەوە و، نهێنی یە و، گرنگە و جێگەی بایەخە، حەجمی کەم دەکەینەوە و زەختی دەخەینەسەر Compressed و، دەیشارینەوە Hidden لەناو فایلێکی تردا.

یەکەم هەنگاو، دۆزینەوە و دیاری کردنی ئەو فایلەی کە دەمانەوێت بەکاری بهێنین بۆ شاردنەوەکە و، دەبێت لە نامە نهێنی یەکە گەورەتر بێت و، ئەم فایلانە پێیان دەوترێت هەڵگر Container یان پەیامبەر و پۆستەچی Carrier کە نامە نهێنی یەکە هەلدەگرێت بۆیە وای پێدەلێن.

هەنگاوی دووا تر، ئەو نامە و پەیامەی دەمانەوێت بیشارینەوە، دەخەینە ناو هەڵگر Embed ((پۆستەچی)) Carrier، بە بەکارهێنانی تەکنیکەکانی ستیگانۆگرافی Steganography Technique.تەکنیکە باوە جیاوازەکان بەکاردەهێنرێت بۆ خستنە ناو و شاردنەوە.

فایلەکانی هەڵگر

Carrier File

فایلە هەڵگرەکان ، کە بەکاردەهێنرێن بۆ لە ستیگانۆ گرافی، دا، ئەمانەی لای خوارەوەن:

- **نووسین و دەق** Text.
- **وێنە** Image (Photo, Picture) .
- **دەنگ** Sound (Audio, Voice).
- **ڤیدیۆ** Video.

چی دەشارێتەوە ...؟؟

What to Hide ...???

ئەوانەی دەتوانین بیانشارینەوە بە گشتی ئەمانەن:

١. **نووسینەکان و دەقەکان** Texts.

٢. **وێنەکان** Images (Photos, Pictures).

٣. **دەنگ** Sound (Audio, Voice).

چۆن بیشارینەوە ...؟؟

How to Hide ... ??

١. **شاردنەوە و خستنەناوی نووسین و دەق** Text **بۆ ناو فایلەکانی** ((**دەق** Text، **وێنە** Image، **دەنگ** Sound)) .

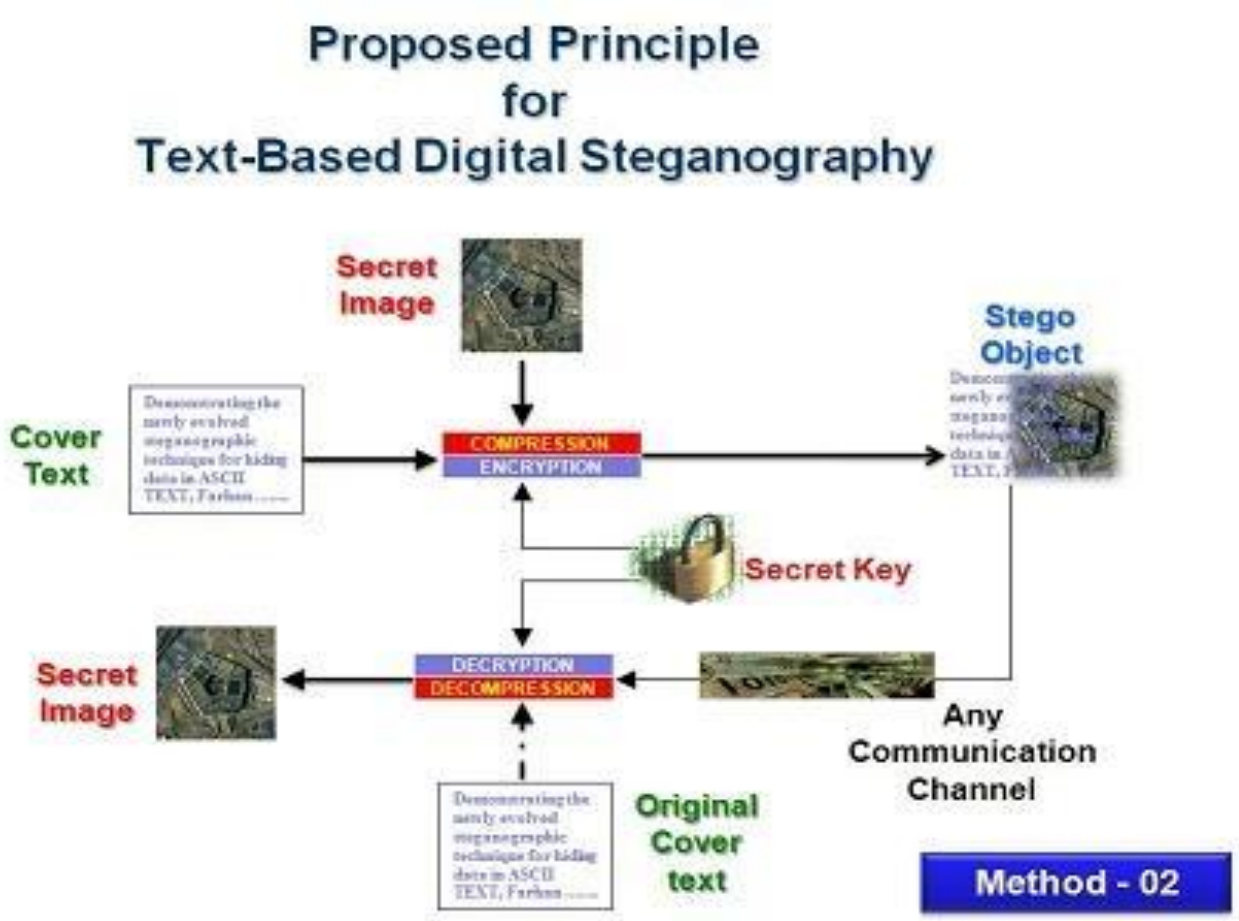
٢. **شاردنەوە و خستنە ناوی وێنە** Image **بۆ ناو فایلەکانی** ((**دەق** Text، **وێنە** Image،

دەنگ Sound)) .

۳. شاردنەوە و خستنە ناوی دەنگ Sound بۆ ناو فایلەکانی ((دەق Text، وێنە Image، دەنگ Sound)) .

بنچینەکانی ستیگانۆگرافی

Basic Principle in Steganography



تەکنیکەکانی ستیگانۆگرافی

Steganography Techniques

ژمارەیەکی زۆر تەکنیك و ڕێگە و شێوازمان هەیە بۆ ستیگانۆ گرافی و، ئیمە لێرەدا تەنها کورتەیەك لەبارەیانەوە دەنووسین و، درێژەیی بابەتەکە هەڵدەگرم بۆ کات و شوێنێکی تر، ئەوانیش:

١. شاردنەوە لە دەق Hiding in Textدا: شاردنەوەی زانیاری لە بەڵگەنامە Document ، بە جێبەجێکردن و چارەسەرکردنی شوێنەکانی دێڕەکان Lines و وشەکان Words، یان شاردنەوەی زانیاری لە فایلی ئێچ تی ئێم ئێڵ دا.

٢. ستیگانۆگرافی جین Genome Steganography: بەکۆد کردنEncoding ی نامە و پەیامی شاراوەیە لە دی ئێن ئەی DNAمرۆڤ دا.

٣. شاردنەوە لە بۆشایی دیسك دا Hiding in the Desk Space: شاردنەوەی زانیاری لە بۆشایی بەکار نەهاتوو Unused Space یان بۆشایی قۆرخکراو ((گیراو)) Reserved.

٤. شاردنەوەی زانیاری لە بەرنامە و سوڕە ئەلیکترۆنیکیەکان Hiding in the Software and Electronic Circuit.

٥. شاردنەوەی زانیاری لە وێنە دا Hiding Information in Image.

٦. شاردنەوە لە پاکەتەکانی ڕایەڵە ((تۆڕ)) دا Hiding in the Network Packets.

شیکارکەری ستیگانۆگرافی

Steganalysis

شیکار کەری ستیگانۆگرافی : بەشێوەیەکی بنچینەیی لێکۆڵینەوەیە لە ناوەرۆکی شاراوە و، کەشف کردنێتی.

ڕێگەکانی کەشفکردنی بەکارهێنانی ستیگانۆ گرافی، بە شێوەیەکی گشتی ئەمانەن:

١. کەشفکردن بە هۆی بینینەوە((ڕوانینیی)) Visual Detection.

٢. کەشفکردنی دەنگ Audible Detection.

٣. کەشفکردنی ئاماری Statistical Detection.

٤. کەشفکرنی پێکهێنەرەکان Structural Detection.بە هۆی بینینی ناوەرۆکەکان و تایبەتمەندی و ڕووخسارەکانی وەکو:

- جیاوازی حەجم Size Difference .
- جیاوازی کات و بەروار Date/ Time Difference.

- گۆڕانی بچووك له ناوەرۆکەکان دا Contents – Modification.

ۆتەرمارکینگ

Watermarking

یەکێکی تره له ڕێگه و هۆیەکانی پارێزگاری Security که لەبارەی جێگیرکردن و دانانی زانیاری و ناسنامەی ناسراوییه ((هەویه)) بۆ مەبەستی پاراستن و، بەکارهێنانی بێ مۆڵەت و ڕێپێنەدراو.

ۆتەرمارکینگی ژمارەیی Digital Watermarking سیگنالی ژمارەیی Digital Signal یه، یان نەخشه Pattern که دادەنرێت و دەخرێته ناو Inserted وێنەی ژمارەیی Digital Image.

نموونەکان

ستیگانۆ گرافی

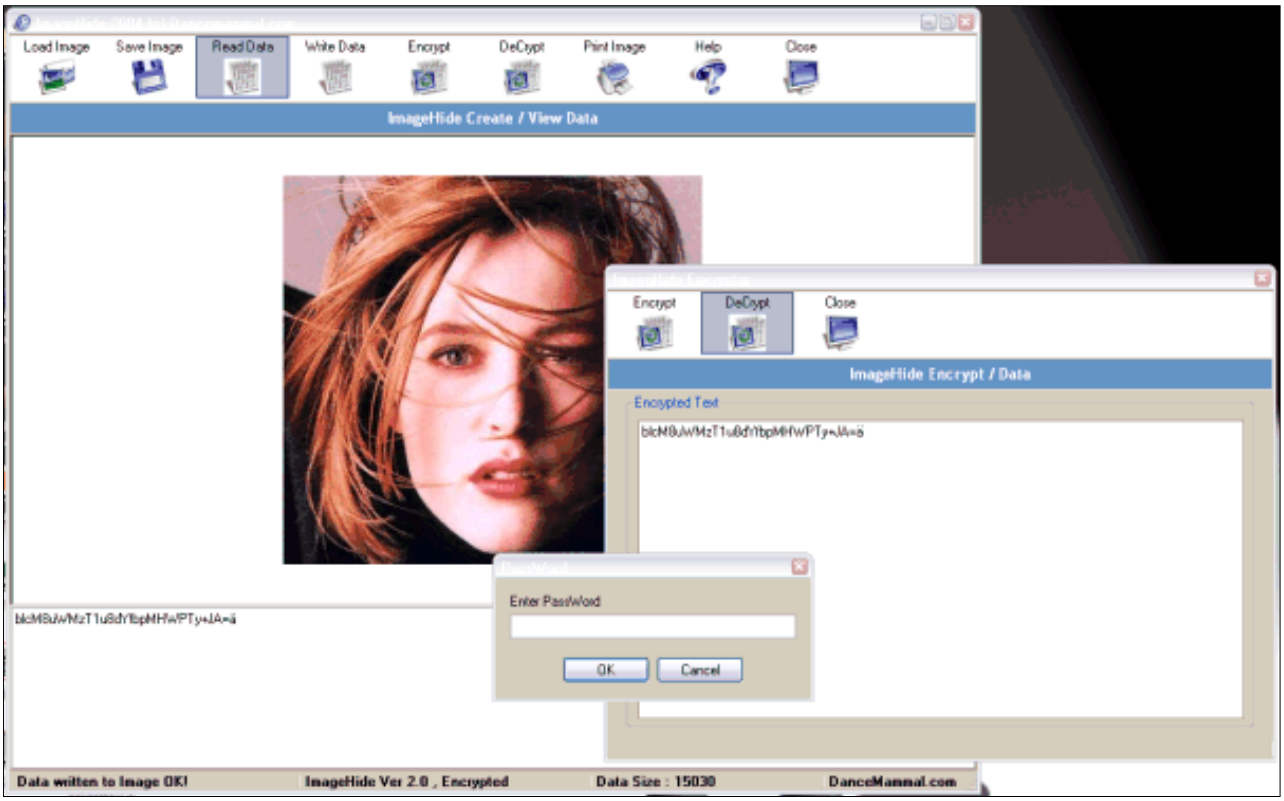
نمونەیەکی زۆر سادە و ئاسان

بەبەکارهێنانی بەرنامەی تایبەت بە بوارەکە

بەرنامەی شاردنەوەی وێنە نەوەی دووەم Image Hide V2.0، یەکێکە لەبەرنامە سادە وساکارە بێ بەرامبەکانی Free Software بواری ستیگانۆ گرافی، کە بەهۆیەوە نمونەیەکی ستیگانۆ گرافی دروست دەکەین و، باشتر لە بابەتی ستیگانۆ گرافی تێدەگەین.

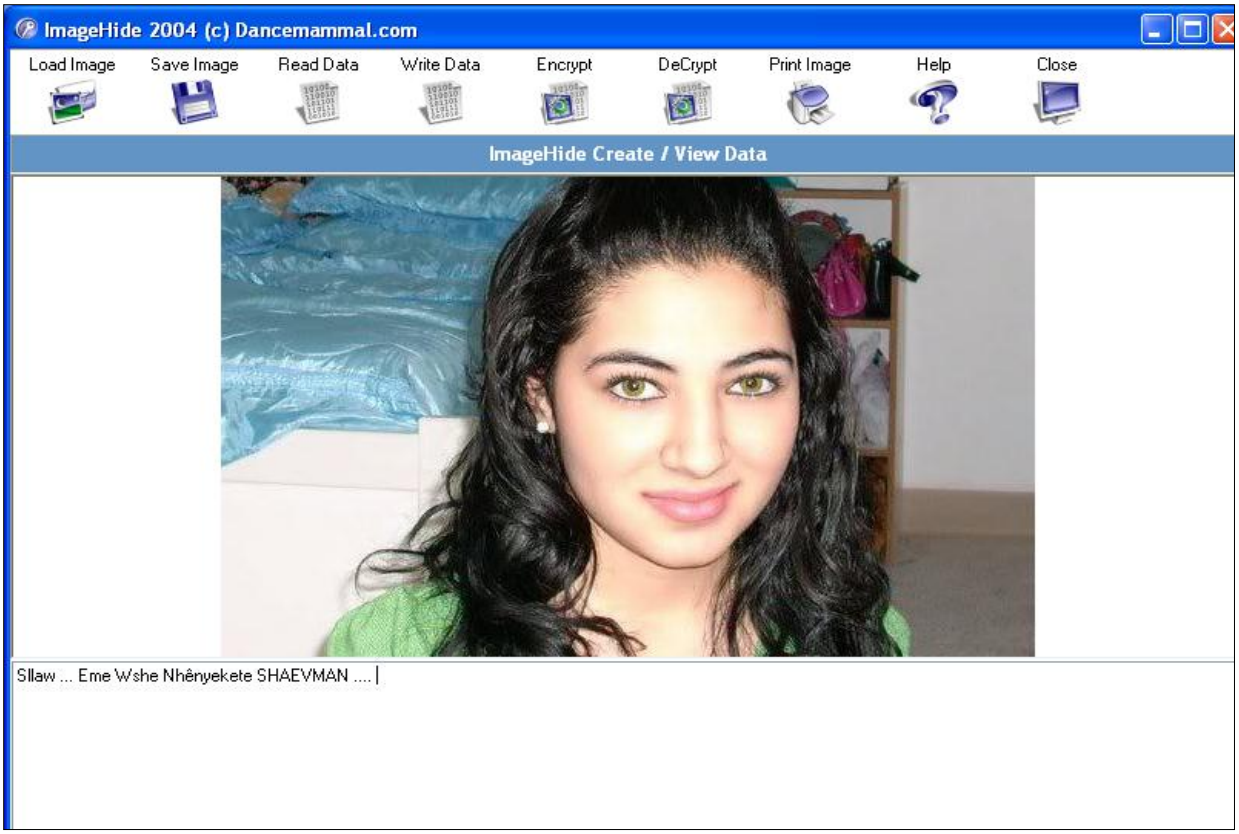
شاردنەوەی تێکست (نووسین) لەناو وێنەیەك دا (ستیگانۆ گرافی)، و بەکۆد کردنی سادە Simple

Encryption بەبەکارهێنانی ڕێگەکانی RC_4 و SHA Hashing، و گۆڕینەوەی ئەو بەکۆد کردنە بۆ شێوەی ئاسایی Decrypt، بێ ئەوەی حەجمی وێنەکە زیادببێت،و وشەنهێنییەکە هاش دەکرێت Hashed Password لە وێنەکەدا و، دەشتوانیت وێنەکە چاپ بکەیت، یان پاشەکەوتی Save بکەیت، بەهەردوو شێوازی BMP یان PNGو، دەتوانیت شێوەی جیاوازی وێنەش بەکاربهێنیت. بەرنامەکەش بەشێوەی بێ بەرامبەر Free دەست دەکەوێت.



هەنگاوەکانی کردارەکە

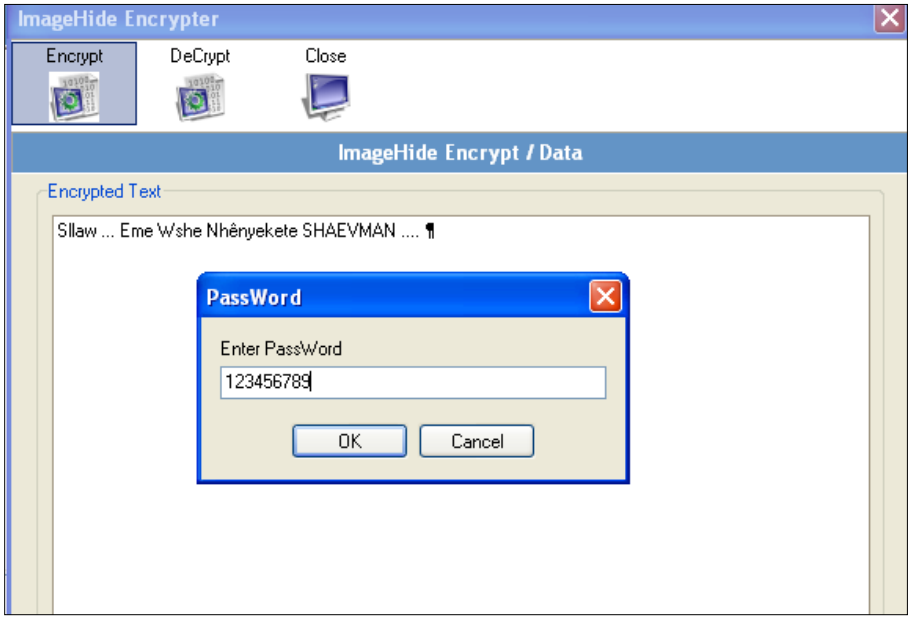
١. بەرنامەکە بکەرەوە.
٢. کلیك لەسەر دووگمەی Lode Image بکە و، وێنەیەك بکەرەوە.
٣. پاشان نووسینەکەت بنووسە .
٤. ئەگەر دەتەوێت ئینکرپیتی بکەیت کلیك لەسەر دووگمەی Encryptبکە:



٥. پاشان کلیك لەسەر دووگمەی Encrypt بکە، لەو پەنجەرەیەی بۆت کراوەتەوە.

٦. وشەیەکی نهێنی داغڵ بکە و، کلیك لەسەر Okبکە.

٧. لەو پەنجەیەی کراوەتەوە کلیك لەسەر دووگمەی Close بکە.



٨. ئێستا وێنەکە چاپ بکە Print، یان پاشەکەوتی Save بکە و بینێرە بۆ هەر شوێنێك کەدەتەوێت.

نمونەی دووەم

کویك ستیگۆ– Quick Stego

یەکەم: بەرنامەی کویك ستیگۆ Quick Stego **دابەزێنە بۆ ناو کۆمپیوتەرەکەت، واتە** Install **ی بکە.**

دووەم: بەرنامەکە بکەرەوە.

سێهەم: کلیك لەسەر دووگمەی Open Image **بکە و، وینەیەك بکەرەوە.**

چوارەم: لە تەنیشتی وێنەکەدا، ئەو نووسینەی هەیە بینووسە .

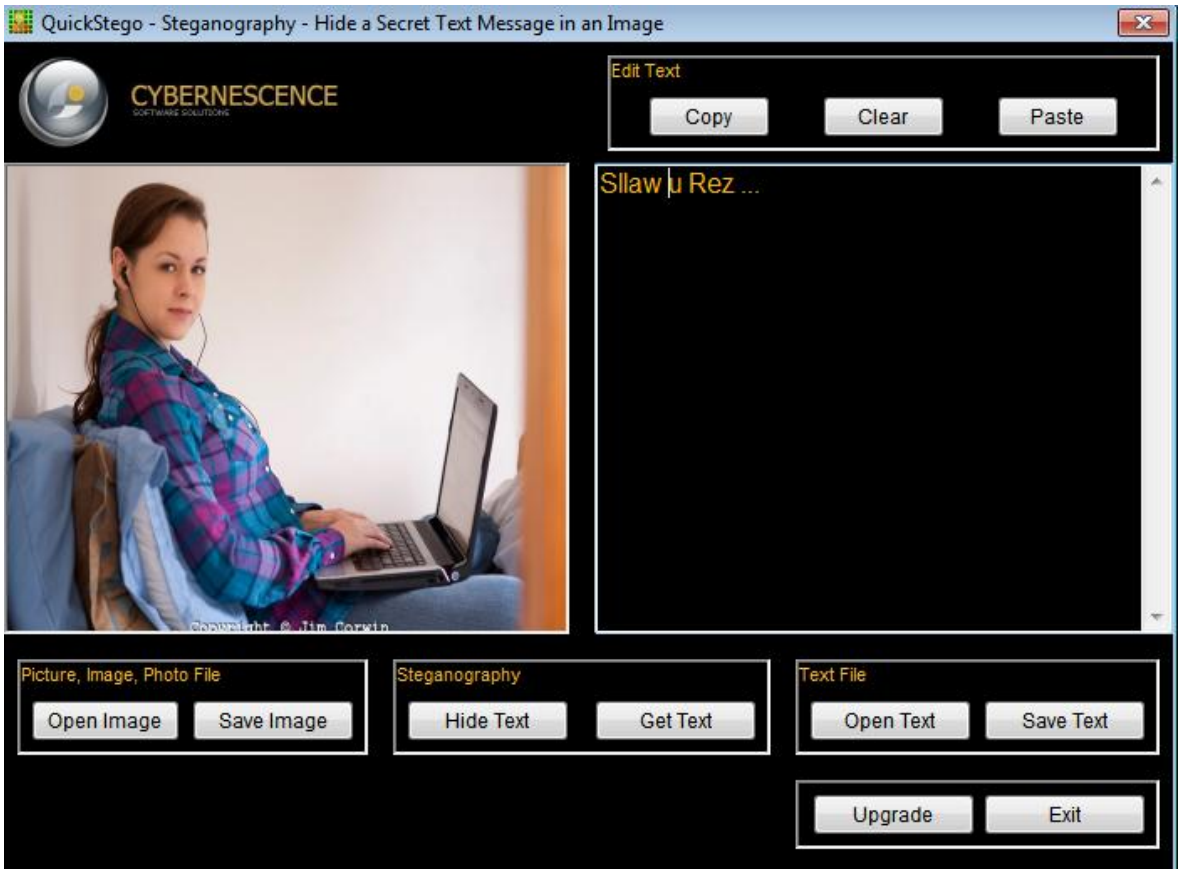
تیبینی:

دەتوانی سوود لە دووگمەکانی بەشی فایلی نووسین Text File **وەربگریت بۆ ئەنجامدانی ئەم کارانەی لای خوارەوە:**

١.دووگمەی Open Text **بۆ هێنان و کردنەوەی نووسینێکی پاشەوت کراو** Save **کە بمانەوێت لەگەڵ وێنەکە بیشارینەوە و دایبنێین.**

٢.دووگمەی Save Text **بۆ خەزنکردن و پاشەکەوت کردنی ئەو نووسینەی خۆمان لە بەشی تەنیشت وێنەکە نووسیمان.**

پێنجەم: دووای ئەوەی نووسینێکت هێنا، یان نووسینێکت نووسی، کلیك لەسەر دووگمەی شاردنەوەی دەق ((نووسین)) Hide Text **بکە، و پاشان کلیك لەسەر دووگمەی** Save Image **بکە بۆ خەزنکردنی وێنەکە.**

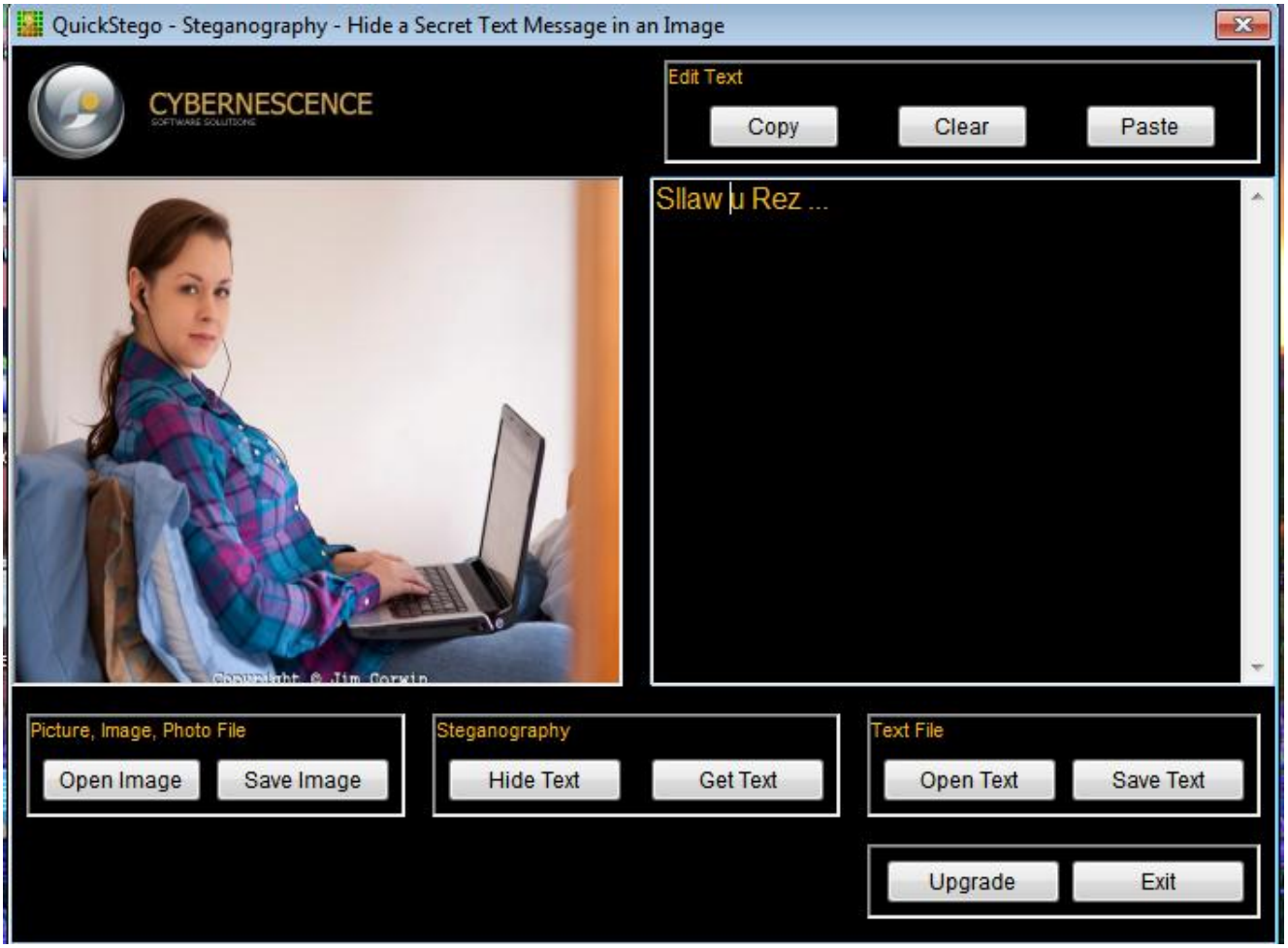


شەشەم: ئەگەر وێنەکە لەگەڵ بەرنامەکانی تر بکەیتەوە جگە لە بەرنامەی کویك ستیگۆ Quick Stigo **ئەوا تەنها وینەکە دەبینی و، بە پێچەوانەشەوە ئەگەر وێنەکە لەگەڵ بەرنامەی کویك ستیگۆ بکەیتەوە، ئەوا دەتوانی وێنەکە و، نووسینەکەش ببینی.**

تیبینی:

١.ئەگەر نووسینەکەی پیشان نەدایت لە تەنیشتی وێنەکەدا، ئەوا کلیك لەسەر دووگمەی Get Text **بکە.**

٢.باری ئاسایشی و پارێزگاری ئەم کارە زۆر بەهێز نییە و تەنها شاردنەوەیە. چونکە یەك تەکنیکی تیا بەکارهاتووە و، ئەویش تەکنیشکی شاردنەوە Hide**یە. بۆیە ریگەکەی پێشوو لە رووی سکیوریتی** Security **یەوە باشترە.**



ۆتەر ماركينگ

Watermaring

یەکەم: بەرنامەی ۆتەر مارك فاکتۆری Watermark Factory دابەزێنە سەر کۆمپیوتەرەکەت، واتە Install ی بکە.

دووەم: پاش دابەزاندن بەرنامە بکەرەوە، Open.

تیبینی: لەبەر ئەوەی بەرنامەکە تۆمار نەکراوە Not Register و کۆدەکەشیمان لانییە بۆیە ناتوانین کۆد داغڵ بکەین Enter Code و بەرنامەکە چالاك بکەین، بۆیە کلیك لەسەر Try Now دەکەین و، بەشێوەیەکی کاتی بەکاری دەهێنین.

سێهەم: فۆڵدەرێك زیاد بکە، بە کلیك کردن لەسەر دووگمەی Add folder و پاشان دیاری کردنی فۆڵدەرەکە لەو رووکارەی بۆت دەکرێتەوە بە کلیك کردن لە سەری و، لە کۆتایدا کلیك لەسەر Ok بکە:

چوارەم: ئەگەر ویستت فایل زیاد بکەیت ((وێنە)) ئەوا کلیك لەسەر Add Files بکە و وینەیەك بهێنە.

پێنجەم: کلیك لەسەر تابی Watermark بکە و، پاشان کلیك لەسەر زیاد کردنی نووسین Add Text بکە و، نووسینێك زیاد بکە.

شەشەم: کلیك لەسەر To Folder بکە و، فۆلدەرێك دیاری بکە بۆ دانانی ئەنجامەکە.

حەوتەم: کلیك لەسەر دووگمەی دروست کردن Generate بکە و، بڕوانە ئەو فۆلدەرەی کە دروستت کرد یان دیاریت کرد بۆ بینینی وینەکان، کە لۆگۆیەك و نووسینێك بۆ هەریەکێك لە وێنەکان زیاد بووە.