O’ZBEKISTAN RESPUBLIKASI BAYLANIS, INFORMATSIYALASTIRIW HA’M TELEKOMMUNIKATSIYA TEXNOLOGIYALARI MA’MLEKETLIK KOMITETI

TASHKENT INFORMATSIYALI’Q TEXNOLOGIYALARI’ UNIVERSITETI NO`KIS FILIALI’

Informatsiyali’q texnologiyalar kafedrasi’

Komp`yuter injiniringi fakul`tetinin` Informatika ha`m informatsiyali’q texnologiyalar bag`dari’ni’n` 4-kurs studenti Jalelova Malikani’n’

PITKERIW QA`NIYGELIK JUMI’SI’

Temasi’: **Mag`li’wmatlardi’ qorg`awdi’n` kriptoalgoritmleri ushi’n programmali’q ta’minat islep shi’g`i’w**

Ilimiy basshi’si’: _________________________ t.i.k. Arzi’mbetov T.Z.

Kafedra basli’g`i’:_________________________ t.i.k. Arzi’mbetov T.Z.

NO`KIS - 2014 j.

MAZMUNI’

Kirisiw ……………………………………………………………………3.

§1. Informatsiyali’q sistemalardi’ jarati’wda del`fi vizual programmalasti’ri’w tiykarlari’ ……………………………………..5

§2. Informatsiyali’q sistemalarda informatsiyani’ qorg`aw ma`seleleri……16

§3.Informatsiyani’ qorg`awdi’n` kriptoalgoritmlik usi’llari’ analizi … …28

§4. Informatsiyalardi’ qorg`awdi’n` kriptografiyali’q usi’li’ni’n` programmali’q qurallari’…………………………………………………42

Juwmaqlaw ………………………………………………………… 49

Paydalani’lg`an a`debiyatlar dizimi …………………………………………50

Qosi’msha

KIRISIW

Ja`miyette avtomatlasti’ri’lg`an informatsiyali’q sistemalardan paydalani’w informatsiyali’q texnologiyalardi’n` qa`wipsizligi da`rejesine baylani’sli’ boladi’. Haqi’yqattanda, komp`yuter sistemalari’ni’n` ken` ko`lemde paydalani’li’wi’ mudami’ ko`beyip o`sip bari’wshi’ informatsiya ko`lemin qollani’w protsessin avtomatlasti’ri’wg`a imkan bersede, bul protseslerdin` agressiv ta`sirlerine qarata g`a`rezli qi’li’p qoyadi’ ha`m informatsiyali’q texnologiyalardan paydalani’wshi’lar aldi’nda jan`a mashqala informatsiyali’q qa`wipsizlik mashqalasi’ ku`ndelikli protsesske aylanadi’.

Qa`wipsizlik mashqalasi’ tiykari’nda jan`a mashqalalardan biri boli’p qalmay, bul qa`wipsizlikti tamiynlew ha`r qanday sistema ushi’n oni’n` quramali’g`i’, tabiyattan qatti’y na`zer birlemshi wazi’ypa esaplanadi’. Biraq qorg`ali’wshi’ ob`ekt informatsiyali’q sistema bolsa, yaki agressiv ta`sir qurallari’ informatsiyali’q formada bolg`anda, qorg`ani’wdi’n` pu`tki`lley jan`a texnologiyalari’n ha`m metodlari’n jarati’wg`a tuwri’ keledi. A’sirese ko`pshilik paydalani’latug`i’n waqti’ bo`liniwshi sistemalarda ha`mde baylani’sti’n` a`piwayi’ telefon liniyasi’ yaki ashi’q komp`yuter tarmaqlari’ arqali’ paydalani’wshi’ sistemalarda qorg`aw qurallari’na bolg`an talap ja`nede joqari’ boladi’. Mag`li’wmatlardi’ qorg`awshi’ metodlar ha`mde xakerlerge qarsi’ ha`reket qurallar kompleksin belgilew maqsetinde komp`yuter qa`wipsizligi qollani’ladi’.

Jumi’sti’n` maqseti informatsiyani’ jetkeriwde qa`wipsizlikti tamiynlewge kiptografiyali’q usi’llardi’ qollani’wg`a qoyi’latug`i’n talaplardi’ tuwri’dan-tuwri’ paydalani’wg`a imkaniyat jarati’p beriwden ibarat.

Qarali’p ati’rg`an pitkeriw qa`nigelik jumi’si’ mag`li’wmatlardi’ qorg`awdi’n` kriptografiyali’q usi’llari’na arnalg`an.

Pitkeriw jumi’si’ 4 paragraftan, kirisiw ha`m juwmaqlaw bo`limleri, a`debiyatlar dizimi ,qosi’mshalardan ibarat.

Jumi’sti’n` kirisiw bo`liminde ma`selenin` tiykarlamasi’ ha`m qurami’ keltirilgen.

Birinshi paragraf informatsiyali’q sistemalardi’n` tiykarg`i’ klassifikatsiyasi’ ha`m ofisti basqari’w usi’llari’ haqqi’ndag`i’ tiykarg`i’ tu`siniklerge arnalg`an.

Ekinshi paragrafta informatsiyali’q sistemalarda informatsiyani’ qorg`awdi’n` teoriyali’q tiykarlari’ ma`selelerin qarap shi’g`i’wg`a arnalg`an.

U`shinshi paragrafta informatsiyani’ qorg`awdi’n` kriptografiyali’q metodlari’na bag`i’shlang`an boli’p, shifrlaw metodlari’ mi’sallar ja`rdeminde teren` bayan etilgen.

To`rtinshi paragrafta informatsiyani’ qorg`awdi’n` kriptografiyali’q metodlari’na Delfi tilinde programma jarati’wg`a bag`i’shlang`an boli’p, a`piwayi’ shifrlaw metodi’na mi’sallar ko`rip shi’g`i’lg`an.

Juwmaqlaw bo`liminde pitkeriw qa`nigelik jumi’si’ni’n` tiykarg`i’ na`tiyjeleri atap o`tiledi.

Qosi’mshada tiyisli programmalar teksti keltiriledi.

§1. Informatsiyali'q sistemalardi' jarati'wda del`fi vizual programmalasti'ri'w tiykarlari'

Delphi de programmalasti'ri'w eki protsesstin` ti'g`i'z o`z-ara ha`reketi menen du`ziledi: programmani'n` vizual ko`rinisin konstruktsiyalaw protsessi (yag`ni'y oni'n` Windows-aynasi') ha`m bul aynani'n` elementlerine programmada kerek wazi'ypani' beriwshi kodti' jazi'w protsessi. Kod jazi'w ushi'n kod aynasi', programmani' konstruktsiyalaw ushi'n Delphi din` basqa aynalari', a`sirese-formalar aynasi' paydalanadi'.

Kod ha`m forma aynalari'ni'n` ta`rkibi arasi'nda ti'g`i'z baylani's boladi'. Bul formag`a komponenttin` jaylasti'ri'li'wi' programma kodi'ni'n` avtomat tu`rde o`zgeriwine ali'p keledi ha`m kerisinshe avtomat tu`rde qoyi'lg`an kod fragmentlerinin` o`shiriliwi sa`ykes komponentlerdin` o`shiriliwine ali'p keletug`i'ni'n an`latadi'. Programmistler da`slep gezektegi komponentti jaylasti'ri'p formani' konstruktsiyalaydi', son` kerek dep tapsa islep turg`an programmada komponenttin` talap etken jag`dayi'n ta`miynleytug`i'n kod fragmentin jazadi'. Sonli'qtan biz Delphi di u`yreniwde programmalasti'ri'wdi' formadan baslaymi'z.

Delphi de jan`a programma menen islep baslag`anda da`slep oni'n` Windows ta normal wazi'ypa ori'nlawi'n ta`miynleytug`i'n minimal kod jarati'ladi'. Solay etip, a`piwayi' programma File | New | Application operatsiyasi'n tan`lag`annan son` da`rriw tayar boladi' ha`m biz programmani' iske qosi'wi'mi'z mu`mkin. Bug`an shekem eki a`hmiyetli na`rse: jeke katalog ashi'w ha`m Delphi di kereginshe sazlaw kerek.

Bul lektsiyada keltirilgen programmalasti'ri'w paketleri menen islew protsessinde formalar ha`m moduller ko`pligin jarati'w kerek boladi'. Bul mag`li'wmatlardi' bo`lek papkada diskli fayllar tu`rinde saqlag`an qolayli'. Bul papkada ha`r bir programma ushi'n o`zinin` ishki papkasi'n jarati'w kerek. Sonda, a`hmiyetli programma ushi'n diskte ori'n aji'rati'w ushi'n sizge tiykarg`i' papkani' joq etiw, al qandayda bir oqi'w programmasi'n birewge beriw ushi'n

disketke sol ishki papkani’ ko`shiriw jekelikti boladi’. Mi’sali’, my_delph atqa iye papka, al onda sizin` birinshi programman`i’z ushi’n ishki papka jarati’n`. Papka ushi’n pgm_1 dep yamasa sog`an uqsas at qoyg`an maqul.

Ekinshi biz Delphi ortali’g`i’ni’n` standart sazlani’wi’na o`zgeris kiritiw ushi’n ne islewimiz kerek. Bul Delphi ortali’g`i’ diskte siz jaratqan programmani’n` son`g`i’ versiyasi’n avtomat tu`rde saqlaw ushi’n kerek.

Tools | Environment options menyu optsiyasi’ tan`lanadi’. Dialog aynada preferences beti boladi’. Shep joqari’ mu`yeshte Autosave | Options topari’nda Editor Files ha`m Desktop o`tkeriwshi boladi’. Bul o`tkeriwshi iske qosi’lsa programmani’n` kod aynasi’ tekstine ha`m Delphi aynalari’ni’n` uli’wma jaylasi’wi’na avtosoxranenie beriledi. Kompilyatsiya izinen baqlaw ushi’n Compiling and Running topari’nda Show Compiler progress o`tkergishin iske qosi’w kerek. Ja`nede programma kodi’nda kommentariylardi’-programma jumi’si’na ta`sir etpeytug`i’n, biraq tekstti tu`siniklirek etetug`i’n fragmentlerdi saqlaw paydali’. Kommentariy rus tilinde paydalanatug`i’n bolsa, programma kodi’n su`wretlew ushi’n sa`ykes shrift tan`lanadi’. Delphi redaktori’nda Courier New shrifti standart turadi’. Onda kirill simvollari’ bolmaydi’. Bul jag`dayda Tools | Editor options optsiyasi’ni’n` Display betinin` Editor Font qatari’nda Courier New Cyr tan`lanadi’ (aldi’ng`i’ versiyalarda Display beti Tools | Environment Options aynasi’nda boladi’).

Endi programmani’ iske tu`siriw ushi’n barli’g`i’ tayar. Tishqansha penen bas aynada knopkasi’ shertilip, F9 basi’ladi’: usi’lay etip Delphi-programma izbe-iz o`z tsikli’nda etapti’ – kompilyatsiya, kompanovka, ori’nlani’w bas etaplari’n o`tedi. Kompilyatsiya etabi’nda kod aynada Object Pascal tilinde tayarlang`an programma tekstin mashinali’ instruktsiyalar izbe-izligine an`lati’w iske asi’ri’ladi’, kompanovka etabi’nda og`an kerek ja`rdemshi programmalar jalg`anadi’, al ori’nlani’w etabi’nda tayar programma operativ yadqa ju`klenedi ha`m og`an ori’nlani’w beriledi.

F9 basi’lsa Delphi Unit1 moduli ushi’n fayl ati’n ha`m ol jaylasqan papkani’ ko`rsetiwdi soraytug`i’n Save Unit1 As dialog ayna payda boladi’. Delphi standart tu`rde modul` fayli’n ha`m proektti BIN sistemali’ papkasi’na jaylasti’ri’wdi’ usi’nadi’.

Delphi rus, frantsuz, kitay ha`m qanday bolsada lati’n alfavitinen basqa simvollardi’ paydalanatug`i’n alfavitti tani’maydi’. Atlar tsifr ha`m belgiler menen baslani’wi’, sondayaq probel mu`mkin emes. Atlar birneshe so`zden ibarat boli’wi’da mu`mkin emes. 8 simvoldan arti’q bolmag`an qi’sqarti’li’w – bul Delphi din` 1-versiyasi’ni’n` sheklewi. Bul versiya uzi’n atlardi’ qabi’llamay tug`i’n Windows Z.x tin` basqari’wi’ asti’nda islewge esaplang`an. Eger siz Delphi 32 penen islesen`iz (yag`ni’y 2 den 6 g`a shekemgi qa`legen versiya), atlardi’ qi’sqartpawi’n`i’zg`a boladi’ ha`m my_first_unit dep yamasa ha`tte moy_pervij_modul dep jazi’wi’n`i’zg`a boladi’, sebebi bul versiyalar fayllarg`a uzi’n atlardi’ paydalani’wg`a mu`mkinshilik beretug`i’n zamanago`y 32-razryadli’ operatsion sistemalarg`a arnalg`an.

Modul` ne ekenligin ani’qlayi’q. Modul` jan`a forma jaratqanda barli’q waqi’tta jarati’ladi’. Delphi programmasi’n kompilyatsiyalawda ha`r bir modul` ushi’n pas, dfm, ocu ken`eytpelerine iye fayllar jarati’ladi’: pas-programma kodi’ aynasi’nan tekst nusqasi’n saqlawshi’ fayl, dfm-ken`eytpeli faylda formalar aynasi’ du`zilisinin` su`wretleniwi saqlanadi’, ocu-faylda eki fayldanda teksttin` mashinali’ instruktsiyag`a aylandi’ri’li’w na`tiyjesi saqlanadi’. ocu fayllari’ kompilyator menen jarati’ladi’. Olardi’ exe ken`etpeli ori’nlawshi’ faylda an`latatug`i’n komponovshik jumi’si’ ushi’n kerek bazani’ beredi.

Programma aynasi’ni’n` zagolovkasi’n o`zgerteyik. Ayna forma menen sa`ykes tu`sedi: Form1. Zagolovkani’ o`zgertiw ushi’n ob`ektler inspektori’ aynasi’n paydalanami’z. Form1 programma aynasi’n jabami’z. Ob`ektler inspektori’ aynasi’nan Caption (Zagolovok) da mi’shti’ shertemiz. Endi bul qatardi’n` Form1 tekstli birinshi kolonkasi’ ren` menen belgilengen ha`m belgilengennen on` jag`i’nda tekstli o`ship-jani’p turi’wshi’ kursor ko`rinedi.

Klaviaturani’ kirillitsani’ kiritiw rejimine o`tkeremiz ha`m «Moya pervaya programma» dep kiritemiz, son` F9 di’ basami’z. Programma «Moya pervaya programma» zagolovkasi’na iye aynani’ jaratadi’.

Solay etip, Ob`ektler inspektori’ aynasi’ qatari’nda a`piwayi’ o`zgeris penen biz a`hmiyetli, programma aynasi’ni’n` qa`siyetlerinen birin-yag`ni’y zagolovkasi’n  o`zgerttik. Formani’n` qa`legen basqa qa`siyetin usi’lay etip o`zgertiwge boladi’.

Formag`a jan`a komponent jaylasti’ri’w qi’yi’nshi’li’q tuwdi’rmaydi’. Buni’n` ushi’n da`slep komponentler politrasi’nan komponent tan`lap, oni’n` shep joqari’ mu`yeshi jaylasi’wi’ kerek bolg`an jerde forma ken`isliginin` jumi’s tochkasi’nan mi’shti’ shertiw kerek.

Programma aynasi’na jazi’wlardi’n` ha`r qi’yli’ tu`rlerin jaylasti’ri’wg`a arnalg`an Label (Metka) komponentin qosi’wdi’ ko`reyik. Komponentler politrasi’nda Standard betin tan`lap, knopkani’ mi’sh` penen shertiw kerek (bul knopka komponentler politrasi’nda Label komponentin su`wretleydi). Endi formag`a mi’shti’ sonday etip shertiw kerek, komponentler formani’n` orayi’nan joqari’raq ha`m shep jaqta jaylasi’wi’ kerek (1.1-su`wret). Formada komponenttin` da`slepki o`lshem ha`m jag`daylari’n mi’sh` penen o`zgertiw an`sat, sonli’qtan su`wrettegidey uqsasli’qqa iye boli’w sha`rt emes.

Jan`a komponent Label1 standart atqa iye boladi’ ha`m ondag`i’ jazi’wda usi’ at penen boladi’. Bul jazi’wdi’ o`zgertiw ushi’n: ob`ektler inspektori’ aynasi’nda Caption qatari’ ja`rdeminde jazi’w kiritemiz: men Delphi de programmalasti’raman. Jan`a jazi’w kiritilgennen formadag`i’ komponent tu`ri o`zgerip baslaydi’.

Jazi’wdi’ ren` menen belgilep, oni’n` shrifti’n irilew qi’lami’z. Bul ushi’n ob`ektler inspektori’ aynasi’nda Font qa`siyeti boyi’nsha mi’shti’ shertip ha`m qatardi’n` on` jag`i’ndag`i’ knopka ja`rdeminde shriftti’ sazlaytug`i’n dialog aynani’ ashami’z. Bul aynani’n` Size (Razmer) diziminde shrift biyikligin

tan`laymi’z, al Color (Tsvet) diziminen kerek ren`di tan`lap, OK knopkasi’ menen aynani’ jabami’z.

1.1-su`wret. Label komponentin jaylasti’ri’w

Delphi formani’ proektlew etabi’ndada komponentler qa`siyetlerinin` qa`lege o`zgerisin vizual iske asi’ra aladi’. Qara tuwri’mu`yeshlik penen jiyeklengen jazi’wdi’n` ishinen mi’shti’ basi’p ha`m oni’n` shep knopkasi’n jabermey turi’p, ko`rsetkishti ayna orayi’ni’n` shep jag`i’na jaylasqansha su`yrep, son` mi’shti’ jiberiw kerek. Usi’lay etip komponentti forma boyi’nsha kerek jag`dayg`a eriskenshe su`yrewge boladi’.

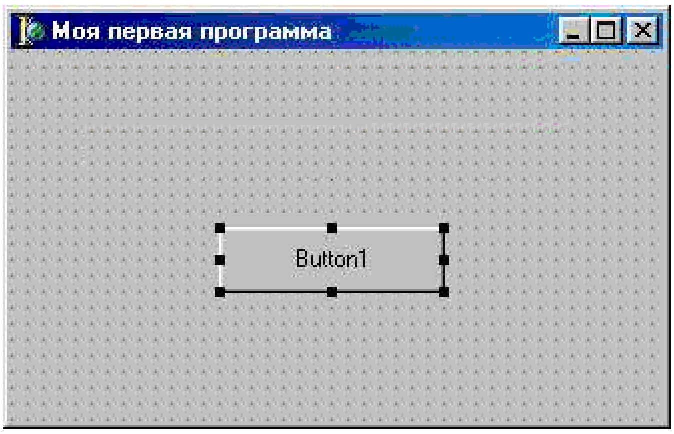
Jiyeklengen qara kvadratlar ja`rdeminde komponent o`lshemin o`zgertiwge boladi’. Biraq ko`rinip turatug`i’n komponentler [ *Delphi de ko`rinetug`i’n ha`m ko`rinbeytug`i’n komponentler paydalanadi’. Ko`rinbeytug`i’n komponentler programmani’ isletiw waqti’nda vizual` su`wretleniwge iye bolmaydi’.*] Left (Sleva), tor (Sverxu), width (Shirina) ha`m Height (Vi’sota) qa`siyetlerine iye boladi’.

Delphi de Left ha`m Tor ma`nisleri komponentti forma boyi’nsha su`yregende mi’sh` ko`rsetkishi jani’nda kishigirim aynada avtomat tu`rde payda boladi’.

Ha`r bir komponent qa`siyetlerden ti’sqari’ ol juwap qaytaratug`i’n waqi’yalar toplami’ menende xarakterlenedi.

Programmag`a modernizatsiya o`tkereyik: og`an bir komponent-knopka- qoyami'z ha`m waqi'yag`a juwap beriwin talap etemiz.

Knopka komponenti komponentler politrasi'ni'n` Standard betinde piktogramma boli'p su`wretlenedi. Bul komponentti formani'n` ortasi'na ha`m belgiden to`menge jaylasti'rami'z (1.2-su`wret).



1.2-su`wret. *Forma so vstavlennoy knopkoy*

Islep turg`an programmada mi'sh` shertilse OnClick waqi'yasi' payda boladi'. Programmani'n` knopkani' basi'wg`a juwap qaytari'wi'n talap etiw Object Pascal tilinde *waqi'yani' islewshi* dep atalatug`i'n programma fragmentin jazi'wi'mi'z kerek. Bul fragment, knopka basi'lg`anda programma ne islewi kerekligin programmist ko`rsetiwi kerek bolg`an tekstli qatarlar izbe-izligine iye boli'wi' kerek. Fragment Object-Pascal tilinin` arnawli' podprogrammasi'-protsedura tu`rinde tayarlanadi'.

Delphi ge OnClick waqi'yasi'n islewshinin` protsedurasi'na tayarlawdi' isletiw ushi'n eki ma`rte izbe-iz mi'shti' jan`a komponentke shertiw kerek. Bunda Delphi kod aynasi'n aktivlendiredi ha`m onda to`mendegishe tekstli fragment boladi':

```
procedure TFormI.ButtonlClick(Sender: TObject);
begin
end;
```

Ol neden ibarat ekenligin ani’qlap ko`reyik. Procedure so`zi protsedura-podprogrammasi’ni’n` baslani’wi’ haqqi’nda kompilyatordi’ ma`limleydi (Delphi de sondayaq funktsiya-podprogrammasi’ paydalanadi’; bul jag`dayda rrocedure so`zinin` orni’na function so`zi paydalanadi’). Son` TForm1.ButtonlClick ati’ keledi. Bul at quramali’: ol TForm1 klasi’ ati’nan ha`m Button1Click protsedurasi’ jeke ati’nan turadi’.

Delphi de klasslar dep programmalardi’n` funktsional juwmaqlang`an fragmentlerine ayti’ladi’. Programmist klass jarati’p ati’ri’p oni’n` ekzemplyari’n sol programmani’n` ha`r qi’yli’ ori’nlari’na yamasa ha`r qi’yli’ programmalarg`a qosi’wi’ mu`mkin. Bunday usi’l programmalasti’ri’wdi’n` maksimal joqari’ o`nimdarli’g`i’n beredi. Delphi qurami’na Borland korporatsiyasi’ni’n` programmistleri jaratqan birneshe ju`zlegen klasslar kiredi. Standart klasslar ji’yi’ndi’si’ bul programmalasti’ri’w sistemasi’ni’n` jaqsi’ mu`mkinshiliklerin ani’qlaydi’.

Ha`r bir komponent qatan` ani’qlang`an klassqa kiredi, al formag`a qoyi’lg`an ani’q komponentler ekzemplyarlari’ sanli’ indeks penen tolti’ri’lg`an klasslar ati’n aladi’. Delphi de paydalani’wi’ boyi’nsha klasslar T ha`ribi menen baslanadi’. Solay etip TForm1, TForm standart klasi’ u`lgisi boyi’nsha jarati’lg`an klass ati’n bildiredi. Kod aynasi’nda tekst basi’nda to`mendegi qatarlar boladi’:

type

Tform1 = class(TForm)

Button1: TButton;

Label1: TLabel;

procedure ButtonlClick(Sender: TObject);

private

{ Private declarations }

public

{ Public declarations }

end;

varForm1: TForm1;

Stroka

TForm1 = class(TForm)

TForm standart klasi'nan du`zilgen TForm1 din` jan`a klassi'n ani'qlaydi' (u`lgi boyi'nsha jarati'lg`an).

Form1: Tform1;

qatarlari' bul klass ekzemplyari'n Form1 ati' menen jaratadi'. TForm1 standart klasi' bos Windows-aynani' su`wretleydi. Bul komponentlerdin` su`wretleniwi to`mendegi qatarlarg`a iye boladi':

Button1: TButton;

Label 1: TLabel;

Bular Button komponenti Tbutton1 standart klassi'ni'n` ekzemplyari' ekenligin, al Label1 komponenti Tlabel klasi' ekzemplyari' ekenligin ko`rsetedi. Tform1. ButtoniSlick protsedurasi' son`i'nda skobkada shaqi'ri'w parametri ko`rinisi keledi:

Sender: Tobject

(Sender parametri Tobject klasi’na kiredi). Protseduralar bir emes, birneshe parametrlerge iye boli’wi’ yamasa uli’wma iye bolmawi’ mu`mkin. Shaqi’ri’w parametrleri (olar bar bolsa) protsedura iske asi’rg`an algoritmnin` konkret jumi’s ori’nlawi’na sazlaw ushi’n xi’zmet etedi. Sender parametri ja`rdeminde Button1Click podprogrammasi’, OnClick waqi’yasi’ qanday komponent jaratqani’n ani’qlawi’ mu`mkin. Barli’q qatar toli’g`i’ menen

procedure TFormI.Buttoniciick(Sender: TObject);

protsedura zagolovkasi’ dep ataladi’. Oni’ «;» simvoli’ juwmaqlaydi’. Bul simvol Object Pascal da a`hmiyetli ori’n tutadi’. Bul-til sistaksisinin` sha`rtli talabi’.

To`mendegi qatarlar protsedura denesin ani’qlaydi’:

begin

end;

begin (nachalo) so`zi protsedura jumi’si’ni’n` algoritmin ta`riypleytug`i’n qosi’mshalar izbe-izliginin` baslani’wi’ haqqi’nda, al end (konets) so`zi bul izbe-izliktin` tamamlani’wi’ haqqi’nda kompilyatorg`a signal beredi. Bizin` jag`dayi’mi’zda protsedura denesi ha`zirshe qadayda bir ha`rekettin` ta`riypleniwine iye emes: Delphi protsedura ushi’n tayarlaw isledi, biraq ol bul protsedurani’n` nege arnalg`ani’n bilmeydi. Deneni kerek qosi’mshalar menen tolti’ri’w-programmisttin` jumi’si’.

Bizge mi’na sha`rt a`hmiyetli, button1 komponentasi’n ha`r bir basqanda basqari’w protsedura denesine beriledi, demek, begin ha`m end so`zleri arasi’nda biz bul waqi’yag`a juwap retinde ori’nlanatug`i’n programma fragmentin jazi’wi’mi’zg`a boladi’.

Bug`an iseniw ushi’n knopkani’ «dawi’sli’» etemiz: begin…end so`zleri arasi’ndag`i’ bos qatarg`a

MessageBeep (MV_OK);

qosi’mshasi’n kiritemiz ha`m komponentlerdin` dawi’s sistemasi’n jalg`ap programmani’ isletemiz. Endi button1 knopkasi’n basqanda juwap retinde komponentler dinamikasi’nda dawi’li’ signal beriledi. Qoyi’lg`an qatar standart protsedurag`a qatnas jasaydi’.

Bizin` programmami’zda button1 knopkasi’ «dawi’sli’» bolg`anli’qtan, oni’n` jazi’wi’n o`zgertemiz: Delphi di komponent ati’ boyi’nsha avtomat tu`rde du`ze alatug`i’n button1 orni’na, mi’sali’, «zvuk» knopkasi’ dep ataymi’z. Buni’ formalar aynasi’ ha`m ob`ektler inspektori’ ja`rdeminde islewge boladi’, yag`ni’y formani’ konstruktsiyalaw etabi’nda, biraq Delphi menen toli’g`i’raq tani’si’w ushi’n biz basqa usi’ldi’ ko`reyik [*Tilekke qarsi’ bul protsedura barli’q waqi’tta isley bermeydi: eger sizin` komp`yuterin`iz dawi’s kartasi’ menen ta`miynlenbegen bolsa, dinamik budet dawi’s shi’g`armaydi’. Bul jag`dayda MessageBeep (MB_OK) orni’na Veer so`zin jazi’n`. Konstruktsiyalaw etabi’nda o`zgeriw statistikali’q dep ataladi’, al programmani’ ori’nlati’w bari’si’nda-dinamikali’q.*] -programmani’ ori’nlati’w etabi’nda jazi’wdi’ dinamikali’q o`zgertiw. Buni’n` ushi’n formag`a OnCreate waqi’yasi’n islewshini jaratami’z.

OnCreate waqi’yasi’ Windows-aynani’ jaratqannan son` payda boladi’, biraq bul ayna ekranda payda bolaman degenshe. Bul waqi’yani’ islewshini jarati’w ushi’n ob`ektler inspektori’ aynasi’ni’n` joqari’si’nda komponentler dizimin ashami’z. Form1 komponentin tan`lap, Events betinde aynani’n` joqari’si’nda OnCreate qa`siyetin mi’sh` penen eki ma`rte shertemiz. Delphi kod aynasi’n jan`adan iske tu`siredi ha`m TForm1. FormCreate protsedurasi’ ushi’n zagotovkani’ ko`rsetedi. Oni’ to`mendegishe redaktorlaymi’z:

procedure TFormi.FormCreate(Sender: TObject);

```
begin
Button1.Caption:= 'Zvuk';
end;
```

Qoyi’lg`an qatar Object Pascal di’n` menshiklew operatori’na iye boladi’. Operatordi’n` shep bo`liminde Button1.Caption qa`siyeti ko`rsetiledi, al on` bo`liminde “zvuk” ma`nisi. Menshiklew operatori’ tochkali’ u`tir menen juwmaqlanadi’.

Button1.Caption quramali’ ati’ kompilyatorg`a jumi’s qaysi’ qa`siyet haqqi’nda boli’p ati’rg`ani’n ani’q ko`rsetiw ushi’n kerek: bizin` programmami’zda ha`r biri Caption qa`siyetine iye 3 komponent paydalanadi’. Qa`siyetke menshiklengen ma`nis tekstli qatar boli’p esaplanadi’. Object Pascal qag`i’ydalari’ boyi’nsha tekstli qatar qorshalg`an apostrof ishinde boli’wi’ kerek. Apostrof ishinde qa`legen mug`darda erkin simvollar jazi’w mu`mkin. Olar knopkada jan`a jazi’wdi’ ani’qlaydi’.

Programmani’n` gezektegi ori’nlani’wi’nan son` knopkada o`zgergen jazi’wdi’ ko`riwge boladi’. Bunnan mi’nanday juwmaq shi’g`ari’w mu`mkin: qa`legen komponenttin` qa`legen qa`siyetin dinamikali’q o`zgertiwge boladi’.

§2. Informatsiyali'q sistemalarda informatsiyani' qorg`aw ma`seleleri

Informatsiyali'q sistemalarda informatsiyani' qorg`aw ma`seleleri to`mendegi bir neshe ko`rinisler boyi'nsha ali'p bari'ladi':

***-Avtomatlasti'ri'lg`an informatsiyali'q sistemalardi' qorg`aw ma`seleleri.*** Informatsiyali'q-kommunikatsiyali'q texnologiyalar tiykari'nan qag`azsi'z avtomatlasti'ri'latug`i'n ha`mde basqari'latug`i'n bolg`anli' sebep, bu`gu`ngi ku`nde informatsiya qa`wipsizligin ta`miyinlew quramalasi'p barmaqta. Soni'n` ushi'nda avtomatlasti'ri'lg`an informatsiyali'q sistemalarda informatsiyani' saqlawdi'n` jan`a zamanagoy texnologiyasi' payda bolmaqta. DataQuest kompaniyasi'ni'n` mag`li'wmati'na qarap, 1996—2000 ji'llarda informatsiyani' qorg`aw programmali'q qurallari'ni'n sati'wdag`i' bahasi' 13 mlrd. AKSh dollarg`a ten` bolg`an.

***- Informatsiyani' qorg`aw sistemalari'.*** Informatsiyani'n` belgili a`zzi ta`replerin kemeytiriwshi ha`m informatsiyag`a kiriwge ruxsat etiwshi, informatsiyani'n` tarqali'p ketiwine ha`m jog`ali'wi'na tosqi'nli'q qi'li'wshi', texnikali'q, programmali'q, texnologiyali'q ha`m jan`a usi'llar kompleksinin` jarati'li'wi'n talap etiledi. Bunday kompleks informatsiyani' qorg`aw kompleksi delinedi.

Informatsiya iyeleri ha`mde wa`kil ag`zalari' tikkeley informatsiyani'n` za`ru`rligin, oni' jog`alti'wdan keletug`i'n zi'yan ha`m qorg`aw mexanizminin` bahasi'nan kelip shi'qqan halda informatsiyani' qorg`awdi'n` za`ru`r da`rejesi ha`m sistemani'n` tu`rin, qurallari'n ani'qlaw za`ru`r. Informatsiyani'n` na`tiyjeligi ha`m talap etiletug`i'n qorg`awdi'n isenimligi bir-biri menen baylani'sli' boladi'.

Qorg`aw sistemasi' u`zliksiz, rejeli, oraylasqan, maqsetli, ani'q isenimli, kompleksli, bekkem ha`m ko`rinisti tez o`zgertetug`i'n boli'wi' sha`rt. Bul a`dette barli'q sharayatlarda bekkem boli'wi' za`ru`r.

***-Ka`rxanalardag`i' informatsiyalardi' qadag`alaw ha`m qorg`aw.*** Informatsiya ko`lemi kishi bolg`an ka`rxanalarda informatsiyani' qorg`awda qolay usi'ldi' qollani'w maqsetke muwapi'q. Ma`selen, oqi'g`an qi'mbat baha qag`azdi' ha`m

elektron xu`jjetti ayri’qsha toparda aji’rati’p toplap, usi’ xu`jjetler menen isleytug`i’n xi’zmetkerdi tayi’nlaw ha`m u`yretiw, basqarmani’ qori’qlawdi’ uyi’mlasti’ri’w, xi’zmetshige kerekli informatsiyani’ tarqatpawdi’ tapsi’ri’w, si’rttan kelgenlerdi qadag`alaw, komp`yuterdi qorg`aw en` tiykarg`i’ ma`sele boli’p tabi’ladi’. Ədetde, qorg`awdi’n` en` kolay usi’li’ sezilerli da`rejede boladi’.

Tiyisli ta`rtipli, ko`p sanli’ avtomatlasti’ri’lg`an informatsiyali’q sistemada ha`m informatsiya ko`lemi joqari’ mekemelerde informatsiyani’ qorg`aw ushi’n qorg`awdi’n` komplekli sistemasi’ qollani’ladi’. Biraq bul usi’l ha`mde qorg`awdi’n` a`dette usi’llari’ xi’zmetkerlerdin` isine ha`dden ti’sqari’ ta`sir jasamawi’ kerek.

-Qorg`aw sistemasi’ni’n` kompleksligi. Qorg`aw sistemasi’ni’n` kompleksligine-informatsiyali’q sistemada xuquqi’y, sho`lkemlestiriw, texnikali’q ha`m programmali’q-matematikali’q zlementlerdin` za`ru`rligi menen erisiledi. Elementler tu`rleri ha`m olardi’n` mazmuni’ ma`kemelerdin` informatsiyani’ qorg`aw sistemasi’ni’n` o`zine tiyisligin ha`m oni’n` ta`kirarlanbawi’n ta`miyinleydi.

Sistema ko`p elementlerden ibarat dep oylaw mu`mkin, onda sistema elementlerinin` mazmuni’ tek oni’n` o`zine, yag`ni’y informatsiyani’n` kerekligine ha`m sistemani’n` o`zin esapqa alg`an belgilengen qorg`aw da`rejesinde ani’qlanadi’.

Informatsiyani’ xuqi’qi’y qorg`aw, elementti qorg`aw jollari’ni’n` tuwri’ ekenligi ma`nisinde ka`rxana ha`m milletlerdin` o`z-ara qatnasi’n yuridikali’q bekkemlew ja`nede personaldi’n` ka`rxanag`a kerekli informatsiyani’ qorg`aw ta`rtibine iseniwi, usi’ ta`rtiptin` buzi’li’wi’na juwapker ekenligi ko`rsetiledi.

-Informatsiyani’ pu`tkilley qorg`aw elementleri: Qorg`aw texnologiyasi’ personaldi’ ka`rxanani’n` kerekli informatsiyani’ qorg`aw qag`i’ydalari’na iseniwi, ori’nlawshi’ basqari’w ha`m shekleniw xarakterine iye bolg`an jag`daylardi’ o`z ishine aladi’.

Pu`tkilley qorg`aw elementi basqa elementlerden o`zgeshe sistemag`a baylani’sti’ri’wshi’ a`mel boli’p esaplanadi’. Ko`pshilik qa`nigelerdin` pikirinshe,

informatsiyani’ qorg`aw sistemasi’ ta`rtibinde pu`tkilley qorg`aw 50-60 %ti qorg`aydi’. Bul ko`pshilik jag`daylarg`a baylani’sli’, sonli’qtan informatsiyani’ pu`tkilley qorg`awdi’n` tiykarg`i’ tu`ri, a`melde qorg`aw printsipine ha`m usi’llari’na ori’nlawshi’ personaldi’ tan`law, jaylasti’ri’w ha`m u`yretiw esaplanadi’.

Informatsiyalardi’ qorg`awdi’n` sho`lkemlestiriw shara-ilajlari’ ka`rxana qa`wipsizligi xi’zmetinin` normativ metodikali’q xu`jjetlerinde o`z ko`rinisin tabadi’. Sol sebepli ko`pshilik jag`daylarda joqari’da ko`rilgen sistema elementlerinin` jalg`i’z ati’-informatsiyani’ sho`lkemlestiriwshilik-huquqi’y qorg`aw elementin paydalani’wdan ibarat.

Informatsiyalardi’ muxandislik-texnikali’q qorg`aw elementi—texnikali’q qurallar kompleksi ja`rdeminde territoriya, ob`ekt ha`m quri’lmalardi’ qorg`audi’ sho`lkemlestiriw ha`mde texnikali’q tekseriw qurallari’na gu`resiw ushi’n mo`lsherlengen. Texnikali’q qorg`aw qurallari’ni’n` bahasi’ joqari’ bolsada, informatsiyali’q sistemani’ qorg`awda bul element belgili a`hmiyetke iye.

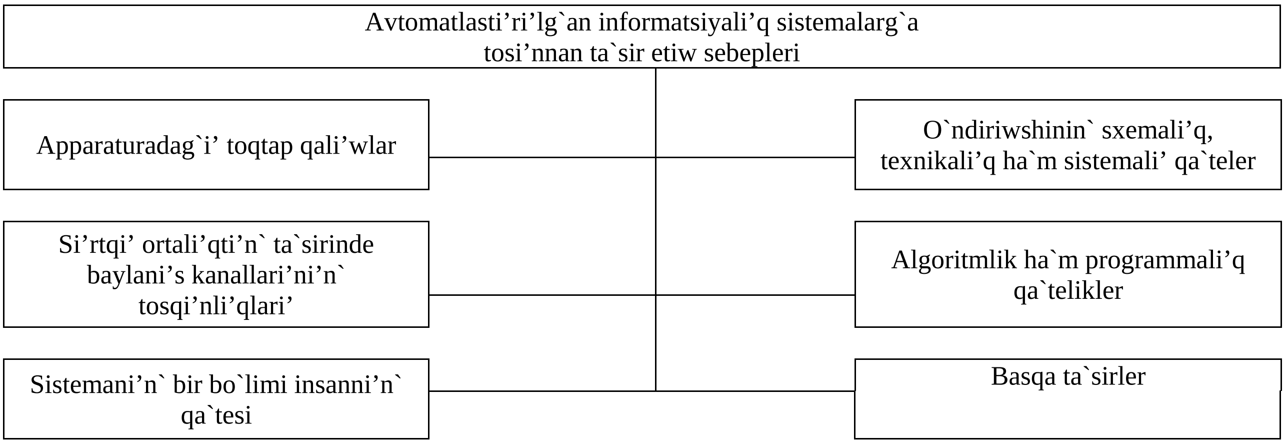
Informatsiyani’ qorg`awdi’n` programmali’q-matematikali’q elementi komp`yuter, lokal tarmaq ha`m tu`rli informatsiyali’q sistemalarda kayta islenetug`i’n, saqlanatug`i’n qi’mbatli’ informatsiyalardi’ qorg`aw ushi’n mo`lsherlengen.

-Informatsiyali’q sistemalarda mag`li’wmatlarg`a qarata qa`wip-qa`terler. Komp`yuter sistemasi’ ha`m tarmag`i’na ziyan keltiriwi mu`mku`n bolg`an sha`rayatta, ha`reket ha`m protsesler komp`yuter sistemasi’ ha`m tarmag`i’ ushi’n *qa`wip-qa`terler* , dep esaplanadi’.

Avtomatlasti’ri’lg`an informatsiyali’q sistemalarg`a tosi’nnan ta`sir ko`rsetiw sebepleri ishine to`mendegiler kiredi (3-su`wret).

Komp`yuter sistemalari’ ha`m tarmaqlari’ni’n` tiykarg`i’ komponentleri-texnikali’q qurallari’, programmali’q-matematikali’q ta`minat ha`m mag`li’wmatlar esaplanadi’. Soni’n` ushi’n teoriyali’q ta`repten bul komponentlerge qarata to`rt tu`rdegi qa`wipler belgili, yag`ni’y u`**ziliw, tuti’p ali’w, o`zgerttiriw ha`m sahtalasti’ri’w:**

**u`ziliw — q**andayda si’rtqi’ ha`reketler (jumi’slar, protsesler)di’ ori’nlaw ushi’n ha`zirgi jumi’slardi’ waqti’nsha orayli’q protsessor quri’lmasi’ ja`rdeminde toqtati’w, olardi’n` ori’nlaytug`i’n son` protsessor aldi’n`g`i’ jag`dayg`a kaytadi’ ha`m tuoqtati’p koyi’lg`an jumi’sti’ dawam etedi. Ha`r bir u`ziliw ta`rtip nomerine iye, onda tiykari’nan orayli’q protsessor quri’lmasi’ qayta islew ushi’n programma bo`legin izlep tabadi’. Protsessorlar eki tu`rdegi u`ziliwler menenn islewdi pada etiwi mu`mku`n: programmali’q ha`m texnikali’q. Birar bir quri’lma tosattan xi’zmet ko`rsetiliwine mu`ta`j bolsa, onda texnik u`ziliw payda boladi’. A`dette bunday u`ziliw orayli’q protsessor ushi’n ku`tilmegen qa`diyse esaplanadi’. Programmali’q u`ziliwler tiykari’nan programmalar ishinde protsessordi’n` belgili buyri’qlari’ ja`rdeminde ori’nlanadi’. Programmali’ buzi’li’wda programma o`z-o`zin waqti’nsha toqtati’p, u`ziliwine belgili protsesti ori’nlaydi’.



3-su`wret. Avtomatlasti’ri’lg`an informatsiyali’q sistemalarg`a tosi’nnan ta`sir ko`rsetiw sebepleri

-tuti’p ali’w protsesi aqi’betinde g`arezsiz shaxslar programmali’q qurallar ha`m informatsiyalardi’n` tu`rli magnitli tasi’wshi’larg`a kiriwdi qolg`a kiritedi. Programma ha`m mag`li’wmatlardan ni’zamsi’z nusxa ali’w, komp`yuter tarmaqlari’ baylani’s kanallari’nan avtorsi’z oqi’wlar ha`m basqada ha`reketler tuti’p ali’w protsesine mi’sal bola aladi’.

**-o`zgerttiriw-** usi’ protses jaman nietli ta`rep tek g`ana komp`yuter sistemasi’ komponentleri (mag`li’wmatlar toplamlari’, programmalar, texnikali’q elementlari) kiriwdi qolg`a kiritedi, balkim olar menen manipulyatsiya (o`zgerttiriw, ko`rinisin o`zgerttiriw)de mu`mku`n. Mi’sali’, o`zgerttiriw

si’pati’nda g`a`rezli ta`reptin` mag`li’wmatlar toplami’ndag`i’ mag`li’wmatlardi’ o`zgerttiriwi, yaki uli’wma komp`yuter sistemasi’ni’n` fayllari’n o`zgerttiriwi, yaki qandayda ni’zamsi’z qayta islewdi a`melge asi’ri’w maqsetinde paydalani’latug`i’n programmani’n` kodi’n o`zgerttiriwi twsiniledi.

- qalbekilestiriw-de protses esaplani’p, oni’n` ja`rdeminde g`a`rezli ta`repler sistemada esapqa ali’nbag`an jag`daylardi’ u`yrenip, ondag`i’ kemshiliklnrdi ani’qlap, keyinshelik o`zine kerakli ha`reketlerdi ori’nlaw maqsetinde sistemag`a kandayda saxta protses yaki sistema da basqa paydalani’wshi’larg`a saxta jazi’wlardi’ jiberedi.

Informatsiyani’ kriptografiyali’q qorg`awdi’n` teoriyali’q tiykarlari’:

Informatsiyani’ kriptografiyali’q qorg`aw degende da`slepki informatsiyani’ sonday o`zgerttiriwlerge ayti’ladi’, na`tiyjede bul informatsiyadan ruxsati’ bolmag`an ta`repler paydalana almaydi’.

Informatsiyani’ kriptografiyali’q o`zgerttiriw metodlari’ni’n` klassifikatsiyalani’wi’nda tu`rli usi’llar bar. Da`slepki informatsiyag`a ta`sir etiw tu`ri boyi’nsha informatsiyani’ kriptografiyali’q o`zgerttiriw metodlari’ni’n` to`mendegi to`rt toparg`a ajrati’w mu`mku`n.

1. Shifrlaw.
2. Steganografiya.
3. Kodlaw.
4. Ori’n almasti’ri’w (zichlashtirish)

Shifrlaw protsesinde da`slepki informatsiya u`stinde qaytari’wshi’li’q qa`siyetine iye bolg`an matematikali’q, logikali’q, kombinatorli’q ha`m basqa o`zgerttiriwler a`melge asi’ri’ladi’. Na`tiyjedea shifrlang`an informatsiya ha`ripler, sanlar, basqa simvollar ha`m ekilik kodlardi’n` ta`rtipsiz naborlari’ ko`rinisin aladi’.

Informatsiyani’ shifrlawda o`zgerttiriw algoritmi ha`m gilt qollani’ladi’. A`dette, shifrlawdi’n` belgili metodi’ ushi’n algoritm o`zgermeydi. Shifrlaw algoritmi ushi’n da`slepki mag`li’wmat si’pati’nda shifrlani’wshi’ informatsiya ha`m shifrlaw giliti xi’zmet etedi. Gilt quri’li’si’na algoritmnin` belgili adi’mi’nda

o`zgerttiriwlerdi ta`miyinlewshi basqari’wshi’ informatsiya ha`mde shifrlaw algoritmin a`melge asi’ri’wda qollani’latug`i’n operandlar kiredi.

Steganografiya metodlari’ tekg`ana saqlani’wshi’ yaki jiberiletug`i’n informatsiyani’n` mazmuni’n, ba`lki qupiya informatsiyani’n` saqlani’wi’ yaki o`tkeriwdi jasi’ri’w imkaniyati’na iye. Bul metodlar tiykari’n ashi’w fayllar arasi’nda qupiya informatsiyani’ maskirovkalawdi’ sho`lkemlestiredi. Komp`yuter sistemalari’nda mul`timediya fayllari’ni’n` paydalani’wi’ steganografiya imkaniyatlari’n ja`nede asi’radi’.

Kodlaw-informatsiyani’ kodlaw degende da`slepki informatsiyani’n` mazmuni’ du`zilisin kodlar menen almasti’ri’w tu`siniledi. Kodlar si’pati’nda ha`riplar, tsifrlar, ha`riplar ha`m tsifrlar birikpeleri isletiliwi mu`mku`n. Kodlawda keri o`zgerttiriwde arnawli’ tablitsalar yaki so`zlerden paydalani’ladi’. Informatsiyani’ kodlawdi’n` mazmun du`zilisi nabori’ shegeralang`an sistemalarda qollani’w maqsetinde muwapi’q esaplanadi’. Qupi’ya informatsiyani’ kodlawda kodlawshi’ tablitsalardi’ saqlawg`a ha`m tarqati’wg`a tuwra keledi.

Uslap qali’ng`an informatsiyani’ statistik metodlar ja`rdeminde islew arqali’ kodlardi’ sezdiriwdin` aldi’n ali’w maqsetinde kodlawshi’ tablitsalardi’ tez-tez o`zgerttirip turi’w lazi’m. Bul qupi’ya informatsiyani’ kodlawdag`i’ kemshilik esaplanadi’.

Informatsiyani’ ori’n almasti’ri’w bazi’ bir sha`rtler menen informatsiyani’ kriptografiyali’q o`zgerttiriwge belgili dep esaplaw mu`mku`n. Ori’n almasti’ri’wdan maqsed informatsiya ko`lemin kemeyttiriw. Ori’n almasti’ri’lg`an informatsiyani’ keri o`zgerttiriwsiz oqi’w yaki onnan paydalani’w mu`mku`n emes. Ori’n almasti’ri’w ha`m keri o`zgerttiriw qurallari’ni’n` paydalani’wshi’li’g`i’ esapqa ali’nsa olardi’ informatsiyani’ kriptografik o`zgerttiriwdegi isenimli qurallar qatari’na qosi’p bolmaydi’. Ha`tteki algoritmler si’r tuti’lg`anda da olar statistik isleniw metodlari’ ja`rdeminde an`sat belgili boli’wi’ mu`mku`n. Sol sebepli ori’n almasti’ri’lg`an qupi’ya informatsiya fayllari’ keyin shifrlanadi’. Waqi’tti’ tejew maqsetinde ori’n almasti’ri’w ha`m shifrlaw protsesi birgelikte a`melge asi’ri’ladi’.

Jeke komp`yuter stenografiyasi'

Ruxsat etilmegen kiriwden informatsiyani' isenimli qorg`aw mashqalasi' a`zelden belgili ha`m ha`zirgi waqi'tqa shekem sheshilmegen. Qupi'ya xabarlardi' jarati'w usi'llari' qadimden belgili, insan xi'zmetinde bul tarawdi' **stenografiya** degen at alg`an. Bul so`z grekcha **Steganos** (qupi'ya, si'r) ha`m **Graphy** (jazi'w) so`zlarinen kelip shi'qqan ha`m «Si'rli' jazi'w» degan ma`nini bildiradi. Stenografiya usi'llari', itimal, jazi'w payda boli'wdan aldi'n payda bolg`an (dastlep sha`rtli belgi ha`m belgilewler qollani'lg`an) boli'wi' mu`mkin.

Informatsiyani' qorg`aw ushi'n **kodlasti'ri'w ha`m kriptografiya** usi'llari' qollani'ladi'.

Kodlasti'ri'w dep informatsiyani' bir sistemadan basqa sistemag`a belgili bir belgiler ja`rdeminde belgilengen ta`rtip boyi'nsha o`tkeriw protsesine ayti'ladi'.

Kriptografiya dep qupi'ya xabar mazmuni'n shifrlaw, yag`ni'y mag`li'wmatlardi' belgili algoritm boyi'nsha o`zgerttirip, shifrlang`an tekstti jarati'w joli' menen informatsiyag`a ruxsat etilmegen kiriwge tosi'q qoyi'w usi'li'na ayti'ladi'.

**Stenografiyani'n`** kriptografiyadan basqa o`zgeshe parqi' da bar. Yag`ni'y oni'n` makseti- qupi'ya xabardi'n` belgili boli'wi'n jasi'ri'w. Bul eki usi'l birlestiriliwi mu`mkin ha`m na`tiyjede informatsiyani' qorg`aw na`tiyjeligin asi'ri'w ushi'n paydalani'li'w imkaniyati' paydo boladi' (mi'sali', kriptografik giltlerdi uzati'w ushi'n).

Komp`yuter texnologiyalari' stenografiyani'n` rawajlani'wi'na ha`m quramalasi'wi'na jan`a tu`rtki berdi. Na`tiyjede informatsiyani' qorg`aw tarawi'nda bag`dar**- kompyuter stenografiyasi** payda boldi'.

Global komp`yuter tarmag`i'ndag`i' ha`m mul`timedia tarawi'ndag`i' zamanago`y progress telekommunikatsiya kanallari'nda mag`li'wmatlarlardi' uzati'w qa`wipsizligin ta`miyinlew ushi'n bag`darlang`an jan`a usi'llardi' jarati'wg`a ali'p keldi. Bul usi'llar shifrlaw quri'lmalari'ni'n` ta`biyiy noani'qli'g`i'nan ha`m analogli' video yaki audiosignallardi'n` kemliginen poydalani'p, xabarlardi' komp`yuter fayllari' (konteynerlar)de jarati'w

imkaniyati’n beredi. Soni’n` menen birge kriptografiyadan par karqli’ tu`rde bul usi’llar informatsiyani’ uzati’w faktinin` o`zin de jaratadi’.

K.Shennon si’rli’ jazi’wdi’n` uli’wma tyooriyasi’n jaratti’, ol pa`n si’pati’nda stenografiyani’n` bazasi’ esaplanadi’. Zamanag`oy komp`yuter steganografiyasi’nda eki tiykarg`i’ fayl tu`rleri belgili: jarati’w ushi’n bag`darlang`an **xabar-fayl, ha`m konteyner-fayl, ol** xabardi’ jarati’w ushi’n paydalani’li’wi’ mu`mkin. Bunda konteynerler eki tu`rde boladi’: **konteyner-original** (yaki «bos» konteyner)- Bul konteyner jasi’ri’n informatsiyani’ saklamaydi’; **konteyner-na`tiyje** (yaki «tolti’ri’lg`an» konteyner)- Bul konteyner jasi’ri’n informatsiyani’ saqlaydi’. **Gilt** si’pati’nda xabardi’ konteynerge kiritip koyi’w ta`rtibin ani’qlaytug`i’n qupi’ya element tu`siniledi.

Komp`yuter stenografiyasi’ rawajlani’wi’

Komp`yuter stenografiyasi’ rawajlani’w tendentsiyasi’ni’n` analizi soni’ ko`rsetedi, keyingi ji’llarda komp`yuter stenografiyasi’ usi’llari’ni’n` rawajlandi’ri’wg`a qi’zi’g`i’w ku`sheyip barmakta. Sonday-aq, belgili, informatsiya qa`wipsizligi mashqalasini’n` aktualli’gi’ mudami’ ku`sheyip barmakta ha`m informatsiyani’ qorg`awdi’n` jan`a usi’llari’n izlew xoshametlenbekte. Basqa ta`repten, informatsiyali’q-kommunikatsiyali’q texnologiyalardi’n` rawajlani’wi’ bul informatsiyani’ qorg`awdi’n` jan`a usi’llari’n usi’ni’w imkani’yatlari’ menen taminlenbekte, bul protsestin` ku`shli katalizatori’ boli’p uli’wma paydalani’latug`i’n Internet komp`yuter tarmag`i’ni’n` ju`da ku`shli rawajlani’wi’ esaplanadi’.

Ha`zirgi waqi’tda informatsiyani’ qorg`aw en` ko`p qollani’latug`i’n taraw bul- kriptografik usi’llar boli’p tabi’ladi’. Lekin, bul jolda komp`yuter viruslari’, «tekstli bomba»lar qusag`an informatsiyali’q qurallardi’n` kriptoqurallardi’ buzatug`i’n ta`sirine baylani’sli’ ko`p sheshiletug`i’n mashqalalar belgili. Basqa ta`repten, kriptografik usi’llardi’ qollani’wda giltlerdi bo`listiriw mashqalasi’ da bu`gu`ngi ku`nde aqi’ri’na shekem sheshilmey tur. Komp`yuter steganografiyasi’ ha`m kriptografiyalari’ni’n` birlestiriliwi payda bolg`an sha`rayatdan quti’li’wdi’n`

jaqsi' bir joli' bolar edi, soni'n` ushi'n bul jag`dayda informatsiyani' qorg`aw usi'llari'ni'n` a`zzi ta`replerin jog`alti'w mu`mkin.

Solay etip komp`yuter stenografiyasi' ha`zirgi ku`nde informatsiya qa`wipsizligi boyi'nsha tiykarg`i' texnologiyalardan biri boli'p esaplanadi'.

Komn`yuter stenografiisini'n` tiykarg`i' wa`ziypalari'

Zamanagoy komp`yuter stenografiyasi'ni'n` tiykarg`i' jag`daylari' to`mendegilerden ibarat:

• jarati'w usi'llari' fayli'ni'n` autentifikatsiyalani'wli'g`i'n ha`m pu`tinligin ta`miyinlewi kerak;

• jaman nietli ta`replerge qollani'li'wshi' steganografiya usi'llari' toli'q belgili dep qaraladi';

• usi'llardi'n` informatsiyaga qarata qa`wipsizlikti ta`miyinlewi ashi'q o`trkeriletug`i'n fayldi'n` tiykarg`i' qa`siyetlerin stenografik almasti'ri'wlar menen saqlawg`a ha`m basqa ta`replerge belgisiz bolg`an qandayda informatsiya - giltke tiykarlanadi';

• Eger jaman niyetli ta`replerge xabardi' ashi'w waqi'ti' belgili boli'p qalg`an bolsa, qupi'ya xabardi'n` o`zin shi'g`ari'p ali'w protsesi quramali' esaplaw ma`selesi si'pati'nda qarali'wi' kerek.

Internet komp`yuter tarmag`i'ni'n` informatsiya dereklerinin` analizi to`mendegi juwmaq shi'g`ari'wg`a imkan berdi, yag`ni'y ha`zirgi waqi'tda stenografik sistemalar to`mendegi tiykarg`i' ma`selelerdi sheshiwde qollani'ladi':

- konfidentsial informatsiyani' ruxsat etilgenmegen kiriwden qorg`aw;
- monitoring ha`m tarmaq zapaslari'n basqari'w sistemalari'n jen`iw;
- programmali'q ta`minatti' ni'qablaw;
- intellektual iyelik etiwdin` ba`zi' bir tu`rlerinde avtorli'k xuqi'qlari'n qorg`aw.

Konfidentsial informatsiyalardi'n` ruxsatsi'z kiriwinen qorg`ani'w

Bul komp`yuter steganografiyasi'n qollani'w tarawi' konfidentsial informatsiyalardi' qorg`aw mashqalasi'n sheshiwde en` na`tiyjeli esaplanadi'. Mi'sali', dawi'sti'n` en` kem a`hmiyetli kishi razryadlari' jasi'ratug`i'n xabarg`a

almasti’ri’ladi’. Bunday o`zgeris ko`pshilik ta`repten dawi’sli’ xabardi’ esitiw payti’nda sezilmeydi.

Monitoring ha`m tarmaq zapaslari’n basqari’w sistemalari’n jen`iw

Sanaat shpionli’q sistemalari’ni’n` monitoringi ha`m tarmoq zapaslari’n basqari’w ha`reketlerine qarsi’ bag`darlang`an stenografik usi’llar lokal ha`m global komp`yuter tarmoqlari’ serverlerinen informatsiyani’n` o`tiwinde qadag`alaw ornati’w ha`reketlerine qarsi’ turiwg`a imkan beredi.

Programmali’q ta`minatti’ ni’qablaw

Komp`yuter steganografiyasi’ni’n` ha`zirgi waqi’tda qollani’latug`i’n basqa bir tarawdi’ programmali’q ta`minatti’ ni’qablaw. Qashandur, programmali’q ta`minatti’ dizimge ali’nbag`an paydalani’wshi’lar ta`repinen paydalani’li’wi’ ori’nsi’z bolsa, ol standart universal programma o`nimleri(mi’sali’, tekstli redaktorlar) asti’nda niqablani’wi’ yaki mul`timedia fayllari’ (mi’sali’, komp`yuter oyi’nlari’ni’n` muzikali’q bo`limi)na jasi’ri’ni’wi’ mu`mkin.

Avtorli’q xuqi’qlardi’ qorg`aw

Stenografiyadan paydalani’latug`i’n ja`ne bir tarawlardan biri- bul avtorli’q huqi’qlari’n qorg`aw esaplanadi’. Komp`yuterli grafik su`wretlerge belgi koyi’ladi’ ha`m ol ko`zge ko`rinbey qaladi’. Lekin, belgili programmali’q ta`minat penen ani’qlanadi’. Bunday programma o`nimi bazi’ jurnallardi’n` komp`yuter versiyalari’nda qollani’li’p ati’r. Stenografiyani’n` bul bag`dari’ tekg`ana su`wretlerdi, ba`lki audio ha`m videoinformatsiyani’ da kayta islewge mo`lsherlengen. Bundan ti’sqari’ oni’n` intellektual iyelik etiwin qorg`awdi’ ta`miyinlew wa`zi’ypasi’ da belgili.

Ha`zirgi waqi’tda komp`yuter stenografiyasi’ usi’llari’ eki tiykarg`i’ bag`dar boyi’nsha rowajbaqta:

- komp`yuter formatlari’ni’n` belgili qa`siyetlerin qollani’wga tiykarlang`an usi’llar;
- audio ha`m vizual informatsiyalardi’n` siyrekligine tiykarlang`an usi’llar.

Stenografik programmalar haqqi’nda qi’sqasha mag`li’wmat

Windows operatsion sistemasi’nda islewshi programmalar:

• Steganos for Win95 programsi’n qollani’w ju`da` jen`il boli’p,  fayllardi’ shifrlaw ha`m olardi’ BMP, DIB, VOC, WAV, ASCII, HTML ken`eytpeli fayllar ishine jaylasti’ri’p jasi’ri’wda ju`da` ku`shli esaplanadi’;

• Contraband programmasi’ 24-bitli VMR formatdag`i grafik fayllar ishinde ha`r qanday fayldi’ jasi’ri’w imkani’yati’na iye.

DOS ortali’g`i’nda islewshi programmalar:

• Jsteg programmasi’ mag`li’wmatlari’ JPG formatli fayllar ishine jarati’w ushi’n mo`lsherlengen;

• FFEncode programmasi’ mag`li’wmatlarlardi’ tekstli fayllar ishinde jarati’w imkaniyati’na iye;

• StegoDOS programmalar paketinin` informatsiyani’ su`wrette jarati’w imkaniyati’ belgili;

• Winstorm programmalar paketi RSX formatli’ fayllar ishine xabardi’ shifrlap jasi’radi’.

OS/2 operatsiyali’q ortali’g`i’nda islewshi programmalar:

- Texto programmasi’ mag`li’wmatlarlardi’ ingliz tilindegi tekstke aylanti’radi’;

- Hide4PGP ch1.1 programmasi’ BMP, WAV, VOC formatli fayllar ishine mag`li’wmatlarlardi’ jarati’w imkaniyati’na iye.

Macintosh komp`yuterleri ushi’n mo`lsherlengen programmalar:

- Paranoid programmasi’ mag`li’wmatlardi’ shifrlap, dawi’sli’ formatli’ fayl ishine jasi’radi’;

- Stego programmasi’ni’n` PICT ken`eytpesi fayl ishine mag`li’wmatlarlar jarati’w imkaniyati’ belgili.

§3. Informatsiyani’ qorg`awdi’n` kriptoalgoritmlik usi’llari’ analizi

«Kriptografiya» atamasi’ da`slep «jasi’ri’w, jazi’wdi’ bekitip koyi’wk» ma`nisin bildirgen. Birinshi ma`rte ol jazi’w payda bolg`an waqi’tlardi’n aq ayti’p o`tilgen. Ha`zirgi waqi’tta kriptografiya degende ha`r qanday formadag`i’, yag`ni’y diskta saqlanatug`i’n sanlar ko`rinisinde yaki esaplaw tarmaqlari’nda o`zati’latug`i’n xabarlar ko`rinisindegi informatsiyani’ jasi’ri’w tu`siniledi. Kriptografiyani’ tsifrlar menen kodlani’wi’ mu`mku`n bolg`an ha`r qanday informatsiyaga qarata qollaw mu`mkin. Qupiyali’qti’ tu`miyinlewge qarati’lg`an kriptografiya ken`rek, kollani’li’w da`rejesine iye. Ani’g`i’raq aytqanda, kriptografiyada qollani’latug`i’n usi’llardi’n` o`zi informatsiyani’ qorg`aw menen baylani’sli’ bolg`an bolg`an ko`p protseslerde paydalani’li’wi’ mu`mkin.

Kriptografiya informatsiyani’ ruxsatsi’z kiriwden qorg`ap, oni’n` si’rli’li’g`i’n ta`miyinleydi. Mi’sali’, to`lew qag`azlari’n elektron pochta arqali’ jetkeriwde oni’n` o`zgerttiriliwi yaki jalg`an jazi’wlardi’n` qosi’li’wi’ mu`mku`n. Bunday jag`daylarda informatsiyani’n` pu`tinligin ta`miyinlew za`ru`rligi payda boladi’. Uli’wma alg`anda komp`yuter tarmag`i’na ruxsatsi’z kiriwdin` pu`tku`lley aldi’n ali’w mu`mku`n emes, lekin olardi’ ani’qlaw mu`mku`n. Informatsiyanin` pu`tinligin tekseriwdin` bunday protsesi, ko`p jag`daylarda, informatsiyani’n` xuqi’qi’yli’g`i’n ta`miyinlew deyiledi. Kriptografiyada qollani’latug`i’n usi’llar ko`p bolmag`an o`zgerttiriwler menen informatsiyalardi’n` haqi’yqi’yli’g`i’n ta`miyinlewi mu`mkin.

Tekg`ana informatsiyani’n` komp`yuter tarmag`i’nan ma`nisi bo`zilmastan kelgenligin biliw, ba`lki oni’n` avtordan kelgenligine isenim payda etiw ju`da za`ru`r. Informatsiyani’ o`tkeriwshi ta`replerni’n` haqi’yqi’yligini tasdiklovchi turli usi’llar belgili. En` universal protsedura parollar menen almasi’w esaplani’p, lekin bul ju`da` na`tiyjeli bolmag`an protsedura boli’p tabi’ladi’. Soni’n` ushi’n paroldi’ qoli’na kiritgen xa`r qanday ta`rep informatsiyadan paydalani’wi’ mu`mkin boladi’. Eger sergeklilik sharalari’na itibar ki’li’nsa, ol jag`dayda parollardi’n` na`tiyjeligin asi’ri’w asi’ri’w ha`m olardi’ kriptografik usi’llar menen qorg`aw

mu`mkin, lekin kriptografiya bundan ku`shlirek, paroldi’ u`zliksiz o`zgerttiriw imkani’n beratug`i’n protsedu ralardi’ da ta`miyinleydi.

Kriptografiya tarawi’ndag`i’ aqi’rg`i’ uti’slardan biri- tsifrli’ signatura - belgili u`lesi menen informatsiyani’ tolti’ri’w ja`rdeminde pu`tinlikti ta`miyinlewshi usi’l, bunda informatsiya oni’n` avtori’ bergen ashi’q gilt belgili bolg`anli’qtan tekseriliwi mu`mkin. Bul usi’l qupi’ya gilt ja`rdeminde pu`tinlik tekseriletug`i’n belgili usi’llardan ko`brek arti’qmashi’li’qlarga iye.

Kriptografiya usi’llari’n qollani’wi’ni’n` ba`zi birlerin ko`rip shi’g`ami’z. O`trkeriletug`i’n informatsiyani’n` ma`nisin jarati’w ushi’n eki tu`rli o`zgerttiriwler qollani’ladi’: **kodlasti’ri’w ha`m shifrlaw.**

Kodlasti’ri’w ushi’n tez-tez qollani’latug`i’n belgiler toplami’n o`z ishine ali’wshi’ kitap yoki tablitsalardan paydalani’ladi’. Bul belgilerden ha`r birine, ko`p jag`daylarda, tsifrlar toplami’ menen beriletug`i’n ixtiyari’y tanlangan kodli’ so`z tuwra keledi. Informatsiyani’ kodlaw ushi’n tap sonday kitap yoki tablitsa talab qi’li’nadi’. Kodlasti’ri’wshi’ kitap yoki tablitsa ixtiyari’y kriptografik o`zgertiriwge mi’sal boladi’. Kodlasti’ri’wdi’n` informatsiyali’q texnologiyasi’na sa`ykes talaplar- qatarli’ belgilerdi sanli’ belgilerge aylanti’ri’w ha`m kerisinshe o`zgerttiriwlerdi ori’nlay biliw. Kodlasti’ri’w kitabi’n tez xa`mde si’rtqi’ yad quri’lmalari’nda a`melge asi’ri’w mu`mkin, lekin bunday tez ha`m isenimli kriptografik sistemani’ barli’q ta`repten tabi’sli’ dep bolmaydi’. Eger bul kitaptan birar ma`rte ruxsatsi’z paydalani’lsa, kodlardi’n` jan`a kitabi’n jarati’w ha`m oni’ barli’q paydalani’wshi’larg`a tarqati’w za`ru`rligi paydo boladi’.

Kriptografik o`zgerttiriwdin` ekinshi tu`ri **shifrlaw** o`z ishine- baslang`i’sh mat` belgilerin ani’qlap oli’w mu`mkin bolmag`an tu`rge o`zgerttiriw algoritmlerin qamrap aladi’. O`zgerttiriwlerdin` bul tu`ri informatsiyali’q-kommunikatsiyali’q texnologiyalarg`a mas keledi.

Bul jerde algoritmdi qorg`aw za`ru`r a`hmiyetli boladi’. Kriptografik giltti qollap, shifrlaw algoritmnin` o`zinde qorg`awg`a bolg`an talaplardi kemeyttiriw mu`mkin. Endi qorg`aw ob`ekti si’pati’nda tek g`ana gilt xi’zmet qi’ladi’. Eger giltten nusqa ali’ng`an bolsa, oni’ almasti’ri’w mu`mkin ha`m bul kodlasti’ri’wshi’

kitap yoki tablitsani’ almasti’ri’wdan jen`il boladi’. Buni’n` ushi’n ha`m kodlasti’ri’w emes, balki shifrlaw informatsiyali’q-kommunikatsiyali’q texnologiyalarda ken` ko`lemli qollani’lmaqta.

Si’rli’ (qupi’ya) baylani’slar tarawi’ **kriptologiya** dep ayti’ladi’. Bul so`z grekshe **«kripto» -** Si’rli’ ha`m **«logus» -** xabar ma`nisin bildiriwshi so`zlerden ibarat. Kriptologiya eki bag`dar, yag`ni’y kriptografiya ha`m kriptoanalizden ibarat.

Kriptografiyani’n` wazi’ypasi’ xabarlardi’n` qupi’yali’g`i’n ha`m haqi’yqi’yli’n`i’n ta`miyinlewdan ibarat.

Kriptoanalizdin` wazi’ypasi’ bolsa kriptograflar ta`repinen islep shi’g`ari’lg`an qorg`aw sistemasi’n ashi’p beriwden ibarat.

Ha`zirgi ku`nde kriptosistemani’ eki klassqa ajrati’w mu`mku`n:

• simmetriyali’ bir giltlilik (qupi’ya giltli);

• asimmetriyali’ eki giltlilik (ashi’q giltli). Simmetriyali’ sistemalarda to`mendegi eki mashqala belgili:

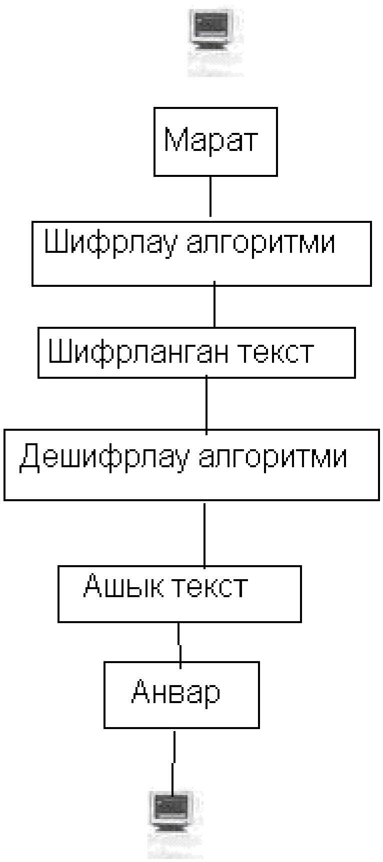
1) Informatsiya almasi’wi’nda qatnasi’wshi’lar sonday jol menen qupi’ya giltti bir-birlerina uzati’wlari’ mu`mku`n?

2) Jiberilgen xabardi’n` xaki’qi’yli’g`i’n qanday ani’qlasa boladi’?

Bul mashqalalardi’n` sheshimi ashi’q giltli sistemalarda o`z ko`rinisin tapti’.

Ashi’q giltli asimmetriyali’ sistemada eki gilt qollani’ladi’. Birinen ekinshisin esaplaw usi’llari’ menen ani’qlap bolmaydi’.

Birinshi gilt informatsiya jiberiwshi ta`repinen shifrlawda qollani’lsa, ekinchisi informatsiyani’ kabi’l qi’li’wshi’ ta`repinen informatsiyani’ tiklewde qollani’ladi’ (4-su`wret) ha`m ol si’r saqlani’wi’ lazi’m.



4-su`wret. Informatsiyani' uzati'w shifrlaw ha`m deshifrlaw

Bul usi'l menen informatsiyani'n` qupi'yali'g`i'n ta`miyinlew mu`mkin. Eger birinshi gilt si'rli' bolsa, ol jag`dayda oni' elektron imza si'pati'nda qollaw mu`mkin ha`m bul usi'l menen informatsiyani' autentifikatsiyalaw, yag`ni'y informatsiyani'n` pu`tinligin ta`miyinlew imkani' payda boladi'.

Informatsiyani' autentifikatsiyalawdan ti'sqari' to`mendegi ma`selelardi' sheshiw mu`mkin:

• paydalani'wshi'ni' autentifikatsiyalaw, yag`ni'y komp`yuter sistemasi' zapaslari'na kiriwshi bolg`an paydalani'wshi'ni' ani'qlaw:

• tarmoq abonentleri baylani'si'n ornati'w protsesinde olardi' o`z-ara autentifikatsiyalaw.

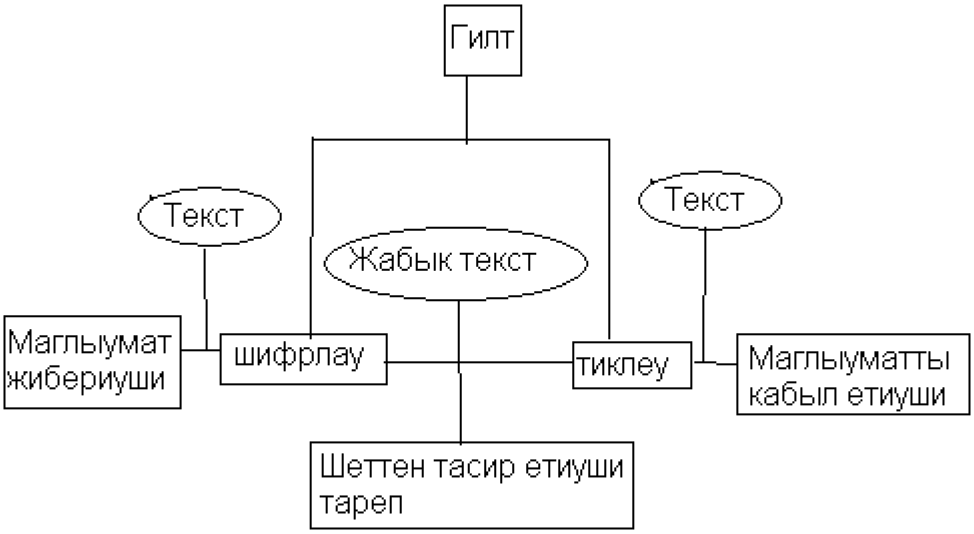
Ha`zirgi ku`nde qorg`ali'wi' za`rur bolg`an bag`darlardan biri bul elektron to`lew sistemalari' ha`m Internet ja`rdeminde a`melge asi'ri'latug`i'n asi'ri'latug`i'n elektron sawdalar esaplanadi'.

Informatsiyalardi’ krintografiyali’ qorg`aw belgileri

Kriptografiya — belgilerin o`zgerttiriw usi’llari’ni’n` toplami’ boli’p, belgilerdi qorg`aw  boyi’nsha to`mendegi eki tiykarg`i’ mashqalalardi’ sheshiwge bag`darlang`an: qupi’yali’q; ani’qli’q.

Qupi’yali’q arqali’ jaman niyetli ta`replerden informatsiyani’ qorg`aw tu`sinilse, **ani’qli’q bolsa** jaman niyetli ta`replerden informatsiyani’ o`zgerttire almasli’q haqqi’nda belgi beredi.

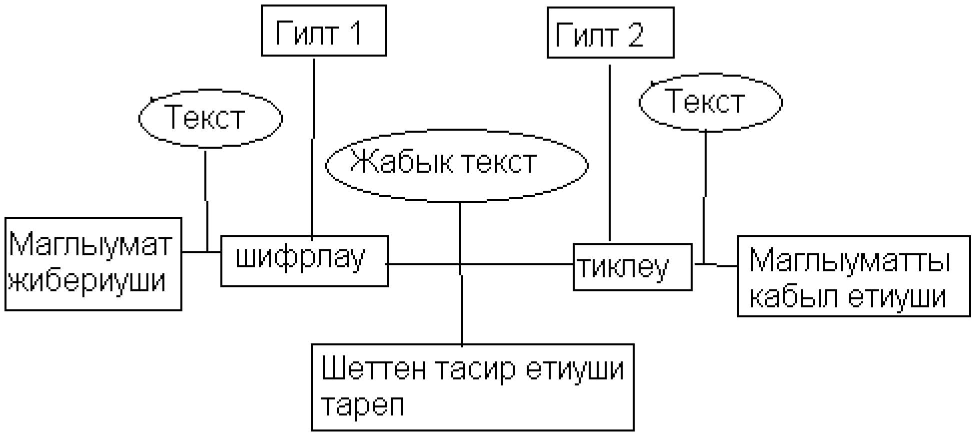
Kriptografiya sistemani’ sxematik ra`wishte to`mendegisha su`wretlew mu`mkin (5-su`wret):



5-su`wret. Kiptografiya sistemasi’ni’n` du`zilisi.

Bul jerde gilt qandayda qorg`alg`an kanal arqali’ jiberiledi (5-su`wrette punktir si’zi’qlar menen ko`rsetilgen). Uli’wma alg`anda bul mexanizm simmetriyali’ bir giltlik sistemag`a kiredi.

Asimmetriyali’ eki giltlik kriptografiya sistemani’ sxematik ra`wishde to`mendegisha su`wretlew mu`mkin (6-su`wret):



6-su`wret. Assimetriyali’ eki giltli kiptografiya sistemasi’ du`zilisi.

Bul jag`dayda qorg`alg`an kanal boyi’nsha ashi’q gilt jiberilip, qupi’ya gilt jiberilmeydi.

Jaman niyetli ta`repler o`z maqsetlerine erise almasa ha`m kriptoanalizshiler giltti bilmesten turi’p, shifrlang`an informatsiyani’ tikley almasa, ol jag`dayda kriptosistema **kriptobekkem sistema** dep ayti’ladi’.

Kriptosistemani’n` bekkemligi oni’n` gilti menen ani’qlanadi’ ha`m bul kriptoanalizdin` tiykarg`i’ qag`i’ydalari’nan biri boli’p esaplanadi’.

Bul ani’qlamani’n` tiykarg`i’ ma`nisi sonnan ibarat, kriptosistema ha`mmege belgili sistema esaplani’p, oni’n` o`zgerttiriliwi ko`p waqi’t ha`m qarejet talap etedi, sol sebepli ha`m tekg`ana giltti o`zgerttirip turi’w menen informatsiyani’ qorg`aw talap etiledi.

Komp`yuter mag`li’wmatlari’n qorg`awdi’n` texnikali’q-programmali’q qurallari’n to`mendegishe 7-su`wrette ko`rsetiw mu`mku`n.

7-su`wret. Komp`yuter mag`li'wmatlari'n qorg`awdi'n` programmali'q qurallari'

1. *Paydalani'wshi'lardi' identifikatsiyalaw ha`m autentifikatsiyalaw sistemasi'.* Bul sistema paydalani'wshi'dan ali'ng`an mag`li'wmatlar boyi'nsha oni'n` ta`repin tekseriw; haqi'yqi'yli'gi'n ani'klaw ha`m keyin og`an sistema menen islewge ruxsat beriw kerekligin belgilep beredi.

Bul jag`dayda tiykari'nan paydalani'wshi'dan ali'natug`i'n belgilerdi tan`law mashqalasi' ani'qlang`an boli'p, oni'n` to`mendegi tu`rlari bar:

- paydalani'wshi'ga belgili bolg`an qupi'ya informatsiya, mi'sali', parol`, qupi'ya gilt ha`m basqalar;
- ta`reptin` fiziologik parametrleri, mi'sali', barmaq izleri, ko`zdin` su`wretlemesi ha`m basqalar.

Birinshisi ku`ndelikli, ekinshisi bolsa biometrik identifikatsiyalaw sistemasi', delinedi.

II. *Disk mag`li'wmatlari'n shifrlaw sistemasi'.* Bul sistemani'n` tiykarg`i' maqseti disktegi *mag`li'wmatlardi'* qorg`aw esaplanadi'. Bul jag`dayda logikali'q ha`m fizikali'q basqi'shlar ajrati'ladi'. Logikali'q basqi'shta fayl tiykarg`i' ob`ekt si'pati'nda boli'p, tek g`ana ba`zi bir fayllar qorg`aladi'. Bunda mi'sal etip, arxivator programmalari'n keltiriw mu`mkin. Fizikali'q basqi'shta disk toli'q qorg`aladi'. Bunda mi'sal si'pati'nda Norton Utilities qurami'ndag`i' Diskreet shifrlawshi' programmani' keltiriw mu`mkin.

*III. Tarmaq boyi’nsha o`trkeriletug`i’n mag`li’wmatlardi’ shifrlaw sistemasi’.* Bul sistemada eki bag`dardi’ ajrati’w mu`mkin:

• kanal boyi’nsha, yag`ni’y baylani’s kanallari’ boyi’nsha u`yreniletug`i’n barli’q mag`li’wmatlarlardi’ shifrlaw;

• abonentler boyi’nsha, yag`ni’y baylani’s kanallari’ boyi’nsha jiberiletug`i’n mag`li’wmatlarlardi’n` tek g`ana mazmun bo`limi shifrlani’p, qalg`an xi’zmetshi mag`li’wmatlarlardi’ ashi’q qaldi’ri’w.

IV. *Elektron mag`li’wmatlardi’ autentifikatsiyalaw sistemasi’.* Bul sistemada tarmoq boyi’nsha ori’nlanatug`i’n elektron mag`li’wmatlar almasi’wi’nda xu`jjetti ha`m oni’n` avtori’n autentifikatsiyalaw mashqalasi’ payda boladi’.

V. *Tayansh informatsiyalardi’ basqari’w qurallari’.* Bul sistemada tayash informatsiyalar si’pati’nda komp`yuter sistemasi’ ha`m tarmag`i’ da qollani’latug`i’n barli’q kriptografik giltler tu`siniledi. Bul jag`dayda giltlardi generatsiyalaw, saqlaw ha`m bo`listiriw usag`an basqari’w funktsiyalari’n ajratadi’.

Simmetriyali’ kriptotizm tiykarlari’

Kriptografiya ko`z-qarastan shifr — Bul gilt dep tu`sinilip ha`m ashi’q mag`li’wmatlarlar toplami’n jabi’q (shifrlang`an) mag`li’wmatlarlarg`a o`zgerttiriw kriptografiya o`zgerttiriwler algoritmleri kompleksi esaplanadi’.

Gilt — kriptografiya o`zgerttiriwler algoritminin` bazi’ bir parametrlerinin` qupi’ya jag`dayi’ boli’p, barli’q algoritmlarden jalg`i’z varianti’n tan`laydi’. Giltlarge qarata qollani’latug`i’n tiykarg`i’ ko`rsetkish boli’p **krintobekkemlik** esaplanadi’.

Kriptografiya qorg`awi’nda shifrlarg`a qarata to`mendegi talaplar koyi’ladi’:

• jeterli da`rejede krintobekkemlik;

• shifrlaw ha`m kodlasti’ri’w protsesinin` a`piwayi’li’g`i’;

• informatsiyalardi’ shifrlaw aqi’betinde olar ko`leminin` arti’p ketpewligi;

• shifrlawdag`i’ kishik qa`telerge ta`sirshen` bolmasli’gi’.

Bul talablarg`a to`mendegi sistemalar juwap beredi:

• ori’nlari’n almasti’ri’w;

• almasti’ri’w;

• gammalasti’ri’w;

• analitik o`zgerttiriw.

Ori’nlari’n almasti’ri’w shifrlaw usi’li’ boyi’nsha baslang`i’sh tekst mag`li’wmatlari’ni’n` teksttin` belgili bir bo`limi shegarasi’nda belgili kag`i’ydalar ja`rdeminde ori’nlari’ almasti’ri’ladi’.

Almasti’ri’w shifrlaw usi’li’ boyi’nsha baslang`i’sh tekst mag`li’wmatlari’ paydalani’li’p ati’rg`an yaki basqa bir alipbe belgilarine almasti’ri’ladi’.

Gammalasti’ri’w usi’li’ boyi’nsha baslang`i’sh tekst mag`li’wmatlari’ shifrlaw gammasi’ belgilari, yag`ni’y tosi’nnan belgiler izbe-izligi menen birlestiriledi.

**Analizli o`zgerttiriw** usi’li’ boyi’nsha baslang`i’sh tekst mag`li’wmatlari’ analitik. formulalar ja`rdeminde o`zgertiriledi, mi’sali’, vektordi’ matritsag`a ko`peytiriw ja`rdeminde. Bul jerde vektor teksttagi mag`li’wmatlar izbe-izligi bolsa, matritsa bolsa gilt si’pati’nda xi’zmet etedi.

Ori’nlardi’ almasti’ri’w usi’llari’

Bul usi’l en` a`piwayi’ ha`m en` da`slepki usi’llar esaplanadi’. ***Ori’nlardi’ almasti’ri’w usi’llari’na*** mi’sal si’pati’nda to`mendegilerdi keltiriw mu`mkin:

- shifrlawshi’ tablitsa; - si’rli’ kvadrat.

Shifrlawshi’ tablitsa usi’li’nda gilt si’pati’nda to`mendegiler qollani’ladi’:

- tablitsa o`lshemleri;

- so`z yaki so`zler izbe-izligi;- tablitsa qurami’ qa`siyetleri.

Mi’sal.

To`mendegi tekst berilgen bolsi’n:

KADRLARDI’ TAYARLAWDI’N` MILLIY DASTURI

Bul informatsiya bag`ana boyi’nsha izbe-iz tablitsaga kiritiledi:

K	L	I’	R	D	I	Y	T
A	A	T	L	I’	L	D	U
D	R	A	A	N`	L	A	R
R	D	Ya	W	M	I	S	I

Na`tijede, 4x8 o`lshemi tablitsa tashkil kilinadi. Endi shifrlangan tekst katorlar boyi’nsha aniklanadi, yag`ni’y o`zimiz ushi’n 4 tadan belgilarni ajratib yozamiz.

KLI’R DIYT AATL I’LDU DRAA N`LAR RDYaW MISI

Bul jerde gilt si’pati’nda tablitsa o`lshewleri xi’zmet etedi.

Bul usi’ldi’ quramalasti’ri’w maqsetinde tayansh so`zdi kiritse boladi’. Joqari’dag`i’ mi’sal ushi’n to`mendegi

ALGORITM

so`zin alami’z ha`m aldi’ngi’ tablitsaga jaylasti’rami’z:

a	l	g	o	r	i	t	m
1	4	2	6	7	3	8	5
K	L	I’	R	D	I	Y	T
A	A	T	L	I’	L	D	U
D	R	A	A	N`	L	A	R
R	D	Ya	W	M	I	S	I

Ekinshi qatardag`i’ tsifrlar ha`riplerdin` alipbe qurami’nan kelip shi’g`adi’. Usi’ qatardag`i’ tsifrlar boyi’nsha bag`analardi’ ta`rtipleymiz:

a	g	i	l	m	o	r	t
1	2	3	4	5	6	7	8
K	I’	I	L	T	R	D	Y
A	T	L	A	U	L	I’	D
D	A	L	R	R	A	N`	A
R	Ya	I	D	I	W	M	S

Shifrlangan tekst to`mendegi ko`riniste boladi’:

KI’IL TRDY ATLA ULI’D DALR RAN`A RYaID IWMS

Si’rli’ kvadrat dep, ketekshelerge 1 den baslap sanlar jazi’lg`an, ondag`i’ ha`r bir bag`ana, qatar ha`m diagonal boyi’nsha sanlar ji’yi’ndi’si’ bir sang`a ten` bolg`an kvadrat formasi’ndag`i’ tablitsag`a ayti’ladi’.

Si’rli’ kvadratqa sanlar ta`rtibi boyi’nsha mag`li’wmatlar kiritiledi ha`m bul mag`li’wmatlar qatarlar boyi’nsha kiritilgende tekst payda boladi’.

Mi’sal.

4x4 o`lshemli si’rli’ kvadratti’ alami’z, bul jerde sanlardi’n` 880 tu`rli kombinatsiyasi’ belgili. To`mendegishe is ali’p barami’z:

16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

Baslang`i’sh tekst si’pati’nda to`mendegi tekstti alami’z:

PROGRAMMALASTI’RI’W TILLERI

ha`m tablitsag`a jaylasti’rami’z:

И	С	А	Л
У	Т	И	А
Ш	Р	Л	Л
Т	Р	А	Д

Shifrlang`an tekst tablitsa elementlarin qatarlar boyi’nsha oqi’w na`tiyjesinde payda boladi’:

ISAL UTIA ShRLL TRAD

Almasti’ri’w usi’llari’

Almasti’ri’w usi’llari’ si’pati’nda to`mendegi usi’llardi’ keltiriw mu`mkin:

— Tsezar usi’li’;

— Affin sistemasi’ndag`i’ Tsezar usi’li’;

— Tayani’sh so`zli Tsezar usi’li’ ha`m basqalar.

Tsezar usi’li’nda almasti’ri’wshi’ ha`ripler k ret ji’lji’w menen ani’qlanadi’. Yuliy Tsezar tuwri’dan-tuwri’ k=3 bolg`anda bul usi’ldan paydalani’lg`an.

K=Z bolg`anda ha`m alipbedegi ha`ripler m=26 ta bolg`anda to`mendegi tablitsa payda etiledi:

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

Mi’sal. Tekst si’pati’nda SAMARQAND so`zin alatug`i’n bolsaq, Tsezar usi’li’ na`tiyjesinde to`mendegi shifrlang`an jazi’w payda boladi’: VDPDUTDQG.

Tsezar usi’li’ni’n` kemshiligi bul bir tu`rli ha`riplerdin`, o`z na`wbetinde, bir tu`rli xa`riplerge almasi’li’wi’.

Affin sistemasi’ndag`i’ Tsezar usi’li’nda ha`r bir ha`ripke almasti’ri’li’wshi’ ha`ripler belgili formula boyi’nsha ani’qlanadi’: at+b (mod m), Bul jerde a,` — pu`tin sanlar, 0< a, b<m, EKUB (a,m)=1.

m=26, a=Z,b=5 bolg`anda to`mendegi tablitsa payda etiledi:

T	0	1	2	3	4	5
Ji+5	5	8	11	14	17	20

6	7	8	9	10	11	12
23	0	3	6	9	12	15

13	14	15	16	17	18	19
18	21	24	1	4	7	10

20	21	22	23	24	25	26
13	16	19	22	25	2	

Usi’g`an uqsas tu`rde ha`ripler to`mendegishe almasti’ri’ladi’.

A	B	C	D	E	F	G	H
F	I	L	O	R	U	X	A

I	J	K	L	M	N	O	P
D	G	J	M	P	S	V	Y

Q	R	S	T	U	V	W	X
B	E	H	K	N	Q	T	W

Y	Z
Z	C

Na`tiyjede joqari’da keltirilgen tekst to`mendegishe shifrlanadi’:

HFPFEBFSO

Tayash so`zli Tsezar usi’li’nda ji’lji’ti’w menen birgelikte tayanch so`z qollani’ladi’. Tayash so`zdi qollani’wdan maqset payda etiletug`i’n alipbede xa`ripler izbea-izligin o`zgerttiriw esaplanadi’.

Mi’sal.

k=5 ha`m DIPLOMAT tayash so`zin alami’z ha`m bul so`z k — ori’nnan jazi’ladi’:

0	1	2	3	4	5	6	7	8	9	10	11	12	13
A	B	C	D	E	F	G	H	I	J	K	L	M	N
					D	I	P	L	O	M	A	T	

14	15	16	17	187	19	20	21	22	23	24	25
O	P	Q	R	S	T	U	V	W	X	Y	Z

Bul tayani’sh so`z a`lipbesindegi ko`rsetilgen ori’nda jaylasti’ri’ladi’, ondag`i’ ha`ripler esapqa ali’nbastan, qalg`an ha`ripler a`lipbedegi ta`rtip boyi’nsha tayani’sh so`zden keyin izbe-iz jazi’ladi’ ha`m na`tiyjede to`mendegi ko`rinis payda etiledi:

0	1	2	3	4	5	6	7	8	9	10	11	12	13
V	W	X	Y	Z	D	I	P	L	O	M	A	T	V

14	15	16	17	187	19	20	21	22	23	24	25
C	E	F	G	H	J	K	N	Q	R	S	U

Joqari’da ko`rip shi’g`i’lg`an SAMARQAND so`zi bolsa belgili usi’l ja`rdeminde HVTVGFVBY g`a o`tkeriledi.

§4. Informatsiyalardi’ qorg`awdi’n` kriptografiyali’q usi’li’ni’n` programmali’q quralları’

I. Ori’nlardi’ almasti’ri’w usi’llari’

1) Shifrlawshi’ tablitsa - si’rli’ kvadrat usi’li’.

Ma`selenin` qoyi’li’wi’:

Qupiyali’q saqlani’wshi’ berilgen so`zdi shifrlawdi’n` N*M o`lshemli kvadrat usi’lda tablitsag`a jaylasti’ri’w.

Mi’sali’: **«Kadrladi’ tayarlawdi’n` milliy programmasi’»** so`zin shifrlaw.

Ma`selenin` sheshiliw algoritmi:

Berilgen so`zdi*** kvadrat usi’lda tablitsag`a jaylasti’ri’wdi’n` ***algoritmi Paskal` tilinde to`mendegishe ta`riplenedi.

O`zgeriwshilerdi ta`riplew bo`limine kiritiledi.

1-etap. Qupiyali’q saqlani’wshi’ berilgen so`z kiritiledi ha`m Paskal` tilinde so`z uzi’nli’g`i’n ani’qlanadi’.

2-etap. So`z uzi’nli’g`i’na qaray berilgen so`zdi shifrlawdi’n` N*M o`lshemli kvadrat usi’lda tablitsag`a jaylasti’ri’w ushi’n «N» ha`m «M» o`lshemlerin Read operatori’ ja`rdeminde soraydi’, usi’ so`z uzi’nli’g`i’ tiykari’nda kvadrat yacheykag`a jaylasatug`i’n o`lshemdi kiritemiz.

Na`tiyjede, eger biz 36 uzi’nli’qtag`i’ so`zge 4*9 matritsasi’n kiritsek onda to`mendegi tablitsag`a iye bolami’z

K	L	I’	R	D	I	Y	G	M
A	A	T	L	I’	L	P	R	A
D	R	A	A	N`	L	R	A	S
R	D	ya	W	M	I	o	M	I’

3-etap.

Matritsag`a jaylasti’ri’lg`an «Kadrladi’ tayarlawdi’n` milliy programmasi’» so`zin jol boyi’nsha oqi’w ha`m na`tiyjede shifrlang`an «KLI’RDIYGMAATLI’LPRADRAAN`LRASRDYaWMIOMI’» so`zi payda etiledi ha`m «N» ha`m «M» o`lshemlerine 0 ma`nisin kiritip matritsa jazi’wi’na

0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0

Iye boladi'.

4-etap. Shifrlang`an «KLI'RDIYGMAATLI'LPRADRAAN`LRASRDYaWMIOMI'» so`zdi ha`m oqi'w ushi'n «N» ha`m «M» o`lshemlerin Read operatori' ja`rdeminde soraladi', shifrlang`an so`z ha`m «N» ha`m «M» o`lshemlerin kiritiledi.

5-etap. Bul etapta programma 36 uzi'nli'qtag`i' so`zde ha`m 4*9 matritsasi'n kiritsek onda qaytadan to`mendegi tablitsag`a iye bolami'z.

K	L	I'	R	D	I	Y	G	M
A	A	T	L	I'	L	P	R	A
D	R	A	A	N`	L	R	A	S
R	D	ya	W	M	I	o	M	I'

6-etap. Programma matritsag`a jaylasti'ri'lg`an mag`li'wmatti' bag`analar boyi'nsha oqi'p bizge da`slepki «Kadrladi' tayarlawdi'n` milliy programmasi'» so`zin keltirip shi'g`ari'p beredi.

2) Si'rli' so`z kiritiw usi'li'.

Ma`selenin` qoyi'li'wi':

Qupiyali'q saqlani'wshi' berilgen so`zdi shifrlawdi'n` si'rli' so`z ja`rdeminde tablitsag`a jaylasti'ri'w.

Mi'sali': «Kadrladi' tayarlawdi'n` milliy programmasi'» so`zin shifrlaw.

Ma`selenin` sheshiliw algoritmi:

Berilgen so`zdi si'rli' so`z tiykari'nda tablitsag`a jaylasti'ri'wdi'n` algoritmi Paskal` tilinde to`mendegishe ta`riplenedi.

O`zgeriwshilerdi ta`riplew bo`limine kiritiledi.

1-etap. Qupiyali'q saqlani'wshi' berilgen so`z kiritiledi ha`m Paskal` tilinde so`z uzi'nli'g`i'n ani'qlanadi'.

2-etap. So`z uzi’nli’g`i’na qaray berilgen so`zdi shifrlawdi’n` si’rli’ so`z tiykari’nda tablitsag`a jaylasti’ri’w ushi’n so`zdi Read operatori’ ja`rdeminde soraydi’, usi’ so`z uzi’nli’g`i’ tiykari’nda kvadrat yacheykag`a jaylasatug`i’n o`lshemdi kiritemiz.

Mi’sali’ si’rli’ so`z si’pati’nda «RING» so`zin paydalansaq, na`tiyjede to`mendegi tablitsag`a iye bolami’z

R	I	N	G
K	T	N	O
A	A	M	G
D	Ya	I	R
R	R	L	A
L	L	L	M
A	A	I	M
R	W	Y	A
D	D	P	S
I’	I’	R	I’

3-etap. Programma «RING» so`zin alfavit tiykari’nda «ginr» so`zge almasti’ri’li’p, tablitsa to`mendegi ko`riniske iye boladi’.

G	I	N	R
O	T	N	K
G	A	M	A
R	Ya	I	D
A	R	L	R
M	L	L	L
M	A	I	A
A	W	Y	R
S	D	P	D
I’	I’	R	I’

4-etap.

Matritsag`a jaylasti'ri'lg`an «Kadrladi' tayarlawdi'n` milliy programmasi'» so`zin jol boyi'nsha oqi'w ha`m na`tiyjede shifrlang`an «GAMARYaIDARLRMLLLMAIAAWYRSDPDI'I'RI'» so`zi payda etiledi ha`m matritsag`a 0 ma`nisin kiritip matritsa jazi'wi'na

0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0

Iye boladi'.

5-etap. Shifrlang`an «GAMARYaIDARLRMLLLMAIAAWYRSDPDI'I'RI'» so`zdi ha`m oqi'w ushi'n si'rli' so`z soraladi' soraladi', shifrlang`an so`z kiritiledi.

6-etap. Bul etapta programma matritsag`a mag`li'wmatti' kiritip to`mendegi tablitsag`a iye bolami'z.

R	I	N	G
K	T	N	O
A	A	M	G
D	Ya	I	R
R	R	L	A
L	L	L	M
A	A	I	M
R	W	Y	A

D	D	P	S
I’	I’	R	I’

7-etap. Programma matritsag`a jaylasti’ri’lg`an mag`li’wmatti’ bag`analar boyi’nsha oqi’p bizge da`slepki «Kadrladi’ tayarlawdi’n` milliy programmasi’» so`zin keltirip shi’g`ari’p beredi.

II. Biz to`mende shifrlawdi’n` a`piwayi’ kriptografik usi’llari’na Del`fi tilinde du`zilgen programmadan paydalani’p programmani’n` islewin tekserip ko`reyik.

Del`fi tilinde du`zilgen programmani’n` proekt kodi’ program Project1 ko`rinisinde boli’p to`mendegi ko`riniske iye.

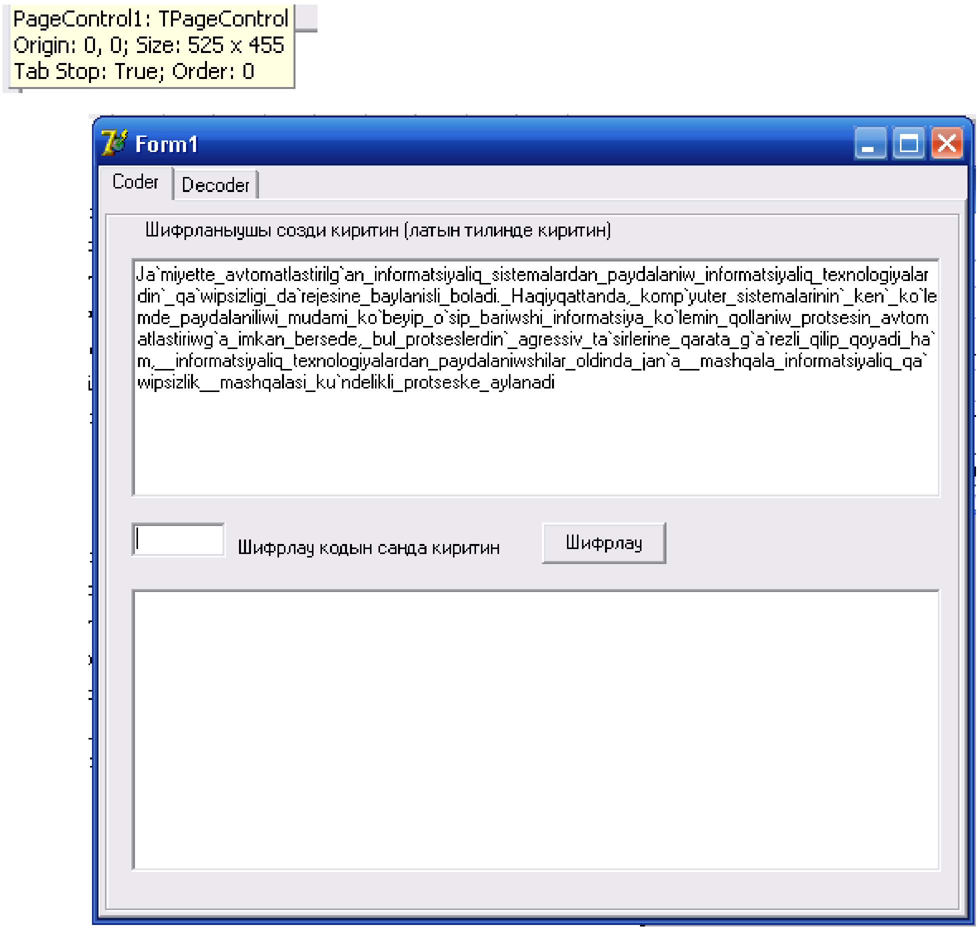
```
program Project1;

uses
  Forms,
  Unit1 in 'Unit1.pas' {Form1};

{$R *.res}

begin
  Application.Initialize;
  Application.CreateForm(TForm1, Form1);
  Application.Run;
end.
```

Al tiykarg`i’ programma qosi’mshada keltiriledi.

Mi’sal: ***«Ja`miyette avtomatlastirilg`an informatsiyaliq sistemalardan paydalaniw informatsiyaliq texnologiyalardin` qa`wipsizligi da`rejesine baylanisli boladi. Haqiyqattanda, komp`yuter sistemalarinin` ken` ko`lemde paydalaniliwi mudami ko`beyip o`sip bariwshi informatsiya ko`lemin qollaniw protsesin avtomatlastiriwg`a imkan bersede, bul protseslerdin` agressiv***

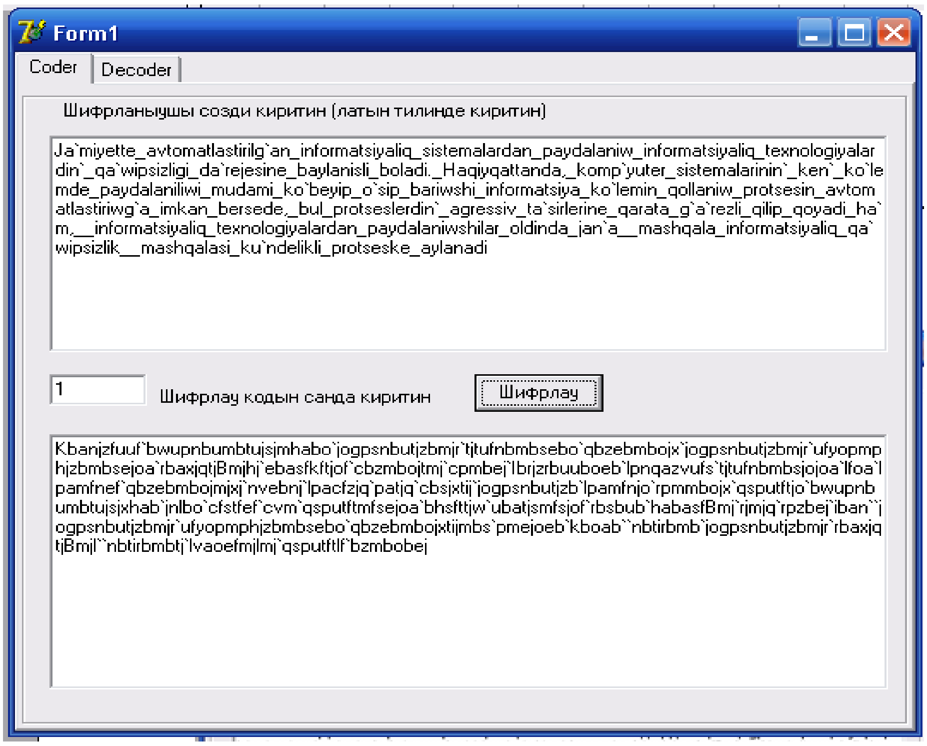
ta`sirlerine qarata g`a`rezli qilip qoyadi ha`m, informatsiyaliq texnologiyalardan paydalaniwshilar oldinda jan`a mashqala informatsiyaliq qa`wipsizlik mashqalasi ku`ndelikli protseske aylanadi».

1-Etap. Bir toli’q pu`tu`n ga`pti “Form1”,“«PageControl1”,“Memo1” maydanshasi’na tomendegishe 4.1-suwrette ko`rsetilgen boyi’nsha kiritemiz.



4.1-suwret. Shifrlani’wshi’ so`zdi kiritiw ko`rinisi.

2-Etap. Shifrlawshi’ so`zdi kiritip boli’p shifr kodi’n sanda kiritiwimiz kerek ha`mde bul sandi’ 1 sani’ menen kiritip «Shifrlau» tuymesin basi’w arqali’ to`mendegi koriniske iye bolami’z.

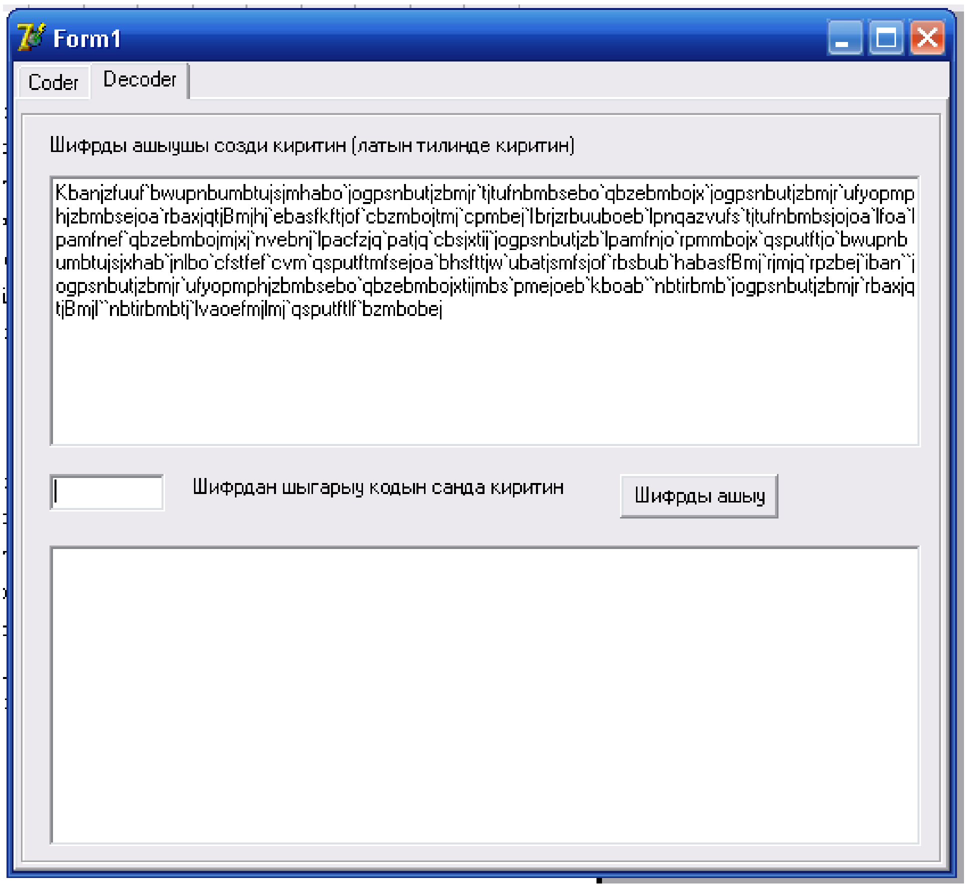


4.2-suwret. Shifrlang`an so`zdi ali’w ko`rinisi.

3-Etap. Bunnan shifrlang`an to`mendegi ko`riniske iye bolg`an so`z payda boldi’.

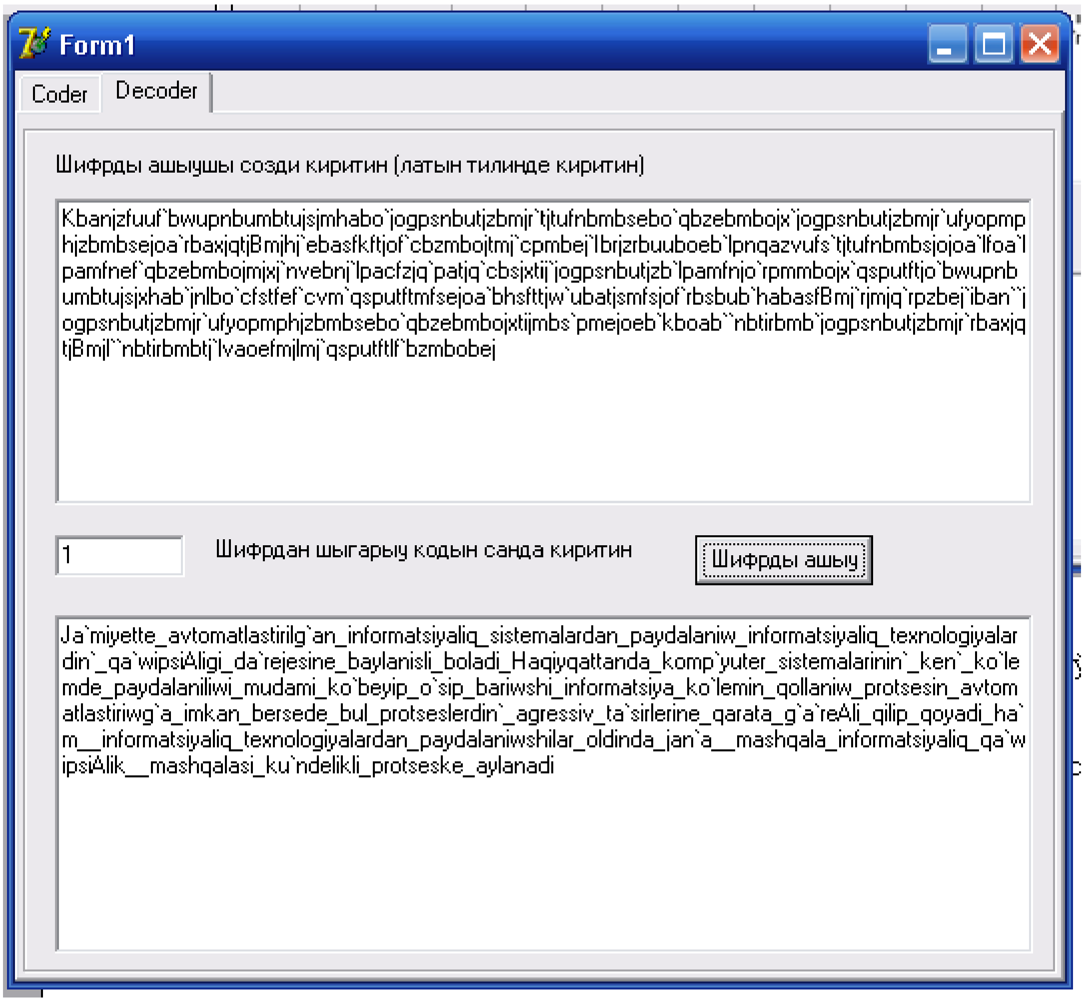
***«Kbanjzfuuf`bwupnbumbtujsjmhabo`jogpsnbutjzbmjr`tjtufnbmbsebo`qbzebmbojx`jogpsnbutjzbmjr`ufyopmphjzbmbsejoa`rbaxjqtjBmjhj`ebasfkftjof`cbzmbojtmj`cpmbej`Ibrjzrbuuboeb`lpnqazvufs`tjtufnbmbsjojoa`lfoa`lpamfnef`qbzebmbojmjxj`nvebnj`lpacfzjq`patjq`cbsjxtij`jogpsnbutjzb`lpamfnjo`rpmmbojx`qsputftjo`bwupnbumbtujsjxhab`jnlbo`cfstfef`cvm`qsputftmfsejoa`bhsfttjw`ubatjsmfsjof`rbsbub`habasfBmj`rjmjq`rpzbej`iban``jogpsnbutjzbmjr`ufyopmphjzbmbsebo`qbzebmbojxtijmbs`pmejoeb`kboab``nbtirbmb`jogpsnbutjzbmjr`rbaxjqtjBmjl``nbtirbmbtj`lvaoefmjlmj`qsputftlf`bzmbobej»*** so`zi payda boldi’. 4.1-suwrette keltirilgen ko`riniste.

4-Etap. Shifrlang`an so`zdi qayta shifrlani’wshi’ so`zge qayta tiklew ushi’n “Form1”,“«PageControl1”,“Memo3”maydanshasi’na tomendegishe 4.3-suwrette ko`rsetilgen boyi’nsha kiritemiz.



4.3-suwret. Shifrlang`an so`zdi kiritiw ko`rinisi.

5-Etap. Shifrlang`an so`zdi kiritip boli’p, shifrlaw waqti’ndag`i’ porol` shifr kodi’n sanda kiritiwimiz kerek. Bul parol kodv 1 edi , buni’ biz 1 sani’ menen kiritemiz ha`mde «Shifrlau» tuymesin basi’w arqali’ to`mendegi ko`riniske iye bolami’z.



4.4-suwret. Shifrdan so`zdi kayta tiklew ko`rinisi.

Bunnan shifrlang`an to`mendegi ko`riniske iye bolg`an so`z payda boldi’. «Ja`miyette_avtomatlastirilg`an_informatsiyaliq_sistemalardan_paydalaniw_informatsiyaliq_texnologiyalardin`_qa`wipsiAligi_da`rejesine_baylanisli_boladi_Haqiyqattanda_komp`yuter_sistemalarinin`_ken`_ko`lemde_paydalaniliwi_mudami_ko`beyip_o`sip_bariwshi_informatsiya_ko`lemin_qollaniw_protsesin_avtomatlastiriwg`a_imkan_bersede_bul_protseslerdin`_agressiv_ta`sirlerine_qarata_g`a`reAli_qilip_qoyadi_ha`m__informatsiyaliq_texnologiyalardan_paydalaniwshilar_oldinda_jan`a__mashqala_informatsiyaliq_qa`wipsiAlik__mashqalasi_ku`ndelikli_protseske_aylanadi» so`zi payda boldi’. 4.4-suwrette keltirilgen ko`riniste.

JUWMAQLAW

Informatsiya almasi'wi'ni'n` mug`dari'ni'n` ko`beyiwi menen informatsiyali'q sistemalarda informatsiyani' saqlawdi'n` jan`a zamanago'y texnologiyasi' payda bolmaqta. Informatsiyani'n` belgili a`zzi ta`replerin kemeytiriwshi ha`m informatsiyag`a kiriwge ruxsat etiwshi, informatsiyani'n` tarqali'p ketiwine ha`m jog`ali'wi'na tosqi'nli'q qi'li'wshi' texnikali'q, programmali'q, texnologiyali'q ha`m jan`a usi'llar kompleksinin` jarati'li'wi'n talap etiledi. Jumi'sti'n` maqseti informatsiyani' jetkeriwde qa`wipsizlikti tamiynlewge kiptografiyali'q usi'llardi' qollani'wg`a qoyi'latug`i'n talaplardi' tuwri'dan-tuwri' paydalani'wg`a imkaniyat jarati'p beriwden ibarat.

Jumi'sti'n` tiykarg`i' na`tiyjeleri retinde to`mendegilerdi ko`rsetip o`tsek boladi':

1. Informatsiyani' qorg`awdi'n` kriptografik usi'llardi' qollani'li'w usi'llari'na qarati'lg`an metodikali'q a`debiyatlardi' u`yreniw.
2. Del`fi programmalasti'ri'w tilinin` mu`mki`nshiliklerin ha`m olardi' programmali'q qurallar jarati'wda qollani'w.
3. Informatsiyani' qorg`awdi'n` kriptografik usi'llari'na qarati'lg`an metodlar ha`m algoritmler menen tani'si'w.
4. Informatsiyani' qorg`awdi'n` kriptografik usi'llari'n sheshiwge qarati'lg`an metodikali'q programmalar qurallar menen tani'si'w.
5. Informatsiyani' qorg`awdi'n` kriptografik usi'llarg`a Del`fi tilinde programmalar qurallar jarati'w.

Pitkeriw qa`niygelik jumi'si'nda islenip shi'g`i'lg`an programmali'q ta`minatti' ken` ko`lemde ha`m ko`p mug`dardag`i' informatsiyani' qorg`aw ushi'n qollansa si'pati'nda paydalansa boladi'.

PAYDALANI’LG`AN A`DEBIYATLAR

1. Simonovich S.V. «Informatika bazovi’y kurs», Sankt —Peterburg: «Piter», 2001 g.
2. Mogilev A.V.,Pak N.I.,Xenner E.K. Informatika. -M.: Akademiya, 2001.
3. Melnikov P.P. Komp`yuterni’e texnologii v ekonomike. Uchebnoe posobie Moskva 2009 g.
4. V.V.Yashenko.Vvedenie v kriptografiyu.Moskva 1998,1999.
5. Parti’ka T.A., Popov I.I. Informatsionnaya bezopasnost` Moskva 2008.
6. Golitsi’na O.L., Popov I.M. Maksimov N.V., Parti’ka T.A.
7. Informatsionni’e texnologii Moskva 2008.
8. Zavgorodniy V.I. Kompleksnaya zashita informatsii v komp`yuterni’x sistemax.Uchebnoe posobie.-M.:PBOYuL N.A.Egorov 2001.264s.
9. Stolins,Vil`yam. Osnovi’ zashit setey.Prilojeniya i standarti’: Per. angl.-M.: Izdatel`skiy dom << Vil`yams >>2002 432s.
10. G`aniev S.K.Karimov M.M xisoblar sistemalariva tarmoqlarida informatsiya ximoyasi: Oliy Wquv yurt.talab.uchun wquv uyullanma-Toshkent davlat texnika universiteti,2003.77.b
11. Vladimir Shupruta. Delphi 2006 na primerax. Uchebnoe posobie. Sankt-Peterburg. 2007. BXV-Peterburg.
12. http://www.ziyonet.uz/

Qosi’msha

```
unit Unit1;

interface

uses
  Windows, Messages, SysUtils, Variants, Classes, Graphics, Controls, Forms,
  Dialogs, StdCtrls, ComCtrls;

type
  TForm1 = class(TForm)
    PageControl1: TPageControl;
    TabSheet1: TTabSheet;
    TabSheet2: TTabSheet;
    GroupBox1: TGroupBox;
    Memo1: TMemo;
    Memo2: TMemo;
    Button1: TButton;
    Edit1: TEdit;
    GroupBox2: TGroupBox;
    RichEdit1: TRichEdit;
    RichEdit2: TRichEdit;
    Edit2: TEdit;
    Button2: TButton;
    Label1: TLabel;
    Label2: TLabel;
    Label3: TLabel;
    Label4: TLabel;
    procedure Button1Click(Sender: TObject);
    procedure Button2Click(Sender: TObject);
```

```
  private
    { Private declarations }
  public
    { Public declarations }
  end;

var
  Form1: TForm1;

implementation

{$R *.dfm}

procedure TForm1.Button1Click(Sender: TObject);
var
  s:string;
  i:integer;
  c,c1:integer;
  key:integer;
  result:string;
begin
s := Memo1.Text;
key := StrToInt(Edit1.text);
for i:=1 to length(s) do
  begin
  c1 := ord(s[i]);
    c1 := c1
  else
    begin
    c1 := c1 + key;
```

```
    end;
  end;

Memo2.Text := result;

end;

procedure TForm1.Button2Click(Sender: TObject);
var
s,result:string;
i,c,key:integer;
begin
s:=RichEdit1.Text;
key:=strtoint(Edit2.Text);

for i:=1 to length(s) do
  begin
  c := ord(s[i]);
      c := c
    else
      begin
        c := c - key;
      end;

  end;
RichEdit2.Text:=result;
end;

end.
```

Tashkent informatsiyali’q texnologiyalari’ universiteti No`kis filiali’ «Komp`yuter injiniringi» fakul`tetinin` «Informatika ha`m informatsiyali’q texnologiyalari’» bag`dari’ni’n` 4-kurs studenti Jalelova Malikani’n’

« Mag`li’wmatlardi’ qorg`awdi’n` kriptoalgoritmleri ushi’n programmali’q ta’minat islep shi’g`i’w» pitkeriw qa`niygelik jumi’si’na

SI’N

Jalelova Malikani’n` si’n berip ati’rg`an, bakalavriatti’ pitkeriw qa`nigelik jumi’si’, ha`zirgi waqi’tta informatsiyali’q sistemalarda informatsiyani’ qorg`aw ma`selesi basli’ ma`selelerdin` biri bolg`anli’qtan, informatsiyali’q qa`wipsizlikti ta`miynlewdegi kiptografiyali’q usi’llardi’ qollani’wg`a qarati’lg`an.

Bul pitkeriw qa`nigelik jumi’si’ kirisiw bo`liminen, to`rt paragraftan, juwmaqlaw bo`liminen ha`m paydalani’lg`an a`debiyatlar diziminen ibarat.

Jumi’sti’n` kirisiw bo`liminde ma`selenin` tiykarlamasi’ ha`m qurami’ keltirilgen.

Birinshi paragraf informatsiyali’q sistemalardi’n` tiykarg`i’ klassifikatsiyasi’ ha`m ofisti basqari’w usi’llari’ haqqi’ndag`i’ tiykarg`i’ tu`siniklerge arnalg`an.

Ekinshi paragrafta informatsiyali’q sistemalarda informatsiyani’ qorg`awdi’n` teoriyali’q tiykarlari’ ma`selelerin qarap shi’g`i’wg`a arnalg`an.

U`shinshi paragrafta informatsiyani’ qorg`awdi’n` kriptografiyali’q metodlari’na bag`i’shlang`an boli’p, shifrlaw metodlari’ mi’sallar ja`rdeminde teren` bayan etilgen.

Juwmaqlaw bo`liminde pitkeriw qa`nigelik jumi’si’ni’n` tiykarg`i’ na`tiyjeleri atap o`tiledi.

Uli’wma alg`anda Jalelova Malika informatsiyali’q qa`wipsizlikti ta`miyinlewde kiptografiyali’q usi’llardi’ qollani’lg`an ha`m Delphi tilinde programma kompleksi du`zilgen.

Juwmaqlap aytqanda, Jalelova Malika bakalavriatti’ pitkeriw qa`nigelik jumi’si’ jaqsi’ ori’nlang`an, qoyi’lg`an talaplarg`a toli’q juwap beredi ha`m «jaqsi’» bahalawg`a i’layi’q dep esaplayman.

Si’n beriwshi f-m.i.kandidati’: dots. R. Mustafaeva