O`ZBEKISTAN RESPUBLIKASI`

XALI`Q BILIMLENDIRIW MINISTIRLIGI

A`JINI'YAZ ATI'NDAG'I' NO'KIS MA'MLEKETLIK PEDAGOGIKALI'Q INSTITUTI'

Qol jazba huquqi'nda

UDK_____

MAGISTRATURA BO'LIMI

INFORMATIKA HA'M XABAR TEXNOLOGIYALARI' KAFEDRASI'

QUNNAZAROV AMANGELDI QUATBAEVICH

Informaciya qa`wipsizligi pa`ni boyi'nsha didaktikali'q materiallar jarati'w

5A110701-Ta`limde xabar texnologiyalari'

Magistr akademiyali'q bilim da`rejesin ali`w ushi`n wori'nlang'an magistirlik

DISSERTATCIYA

Ilimiy basshi`: **f.m.i.k. doc: Tureniyazova A.**

No'kis-2014

MAK g’a jaqlawg’a ruxsat yetilgen

Magistratura bo’limi basli’g’i’:_____ f.m.i.k. doc.Atashov B.T.

Kafedra basli’g’i’:_____ f.m.i.k. doc:Tureniyazova A.I.

Ilimiy basshi’:_____ f.m.i.k. doc:Tureniyazova A.I.

MAGISTRLIK DISSERTATCIA JUMI’SI’

Ajiniyaz ati’ndag’i’ No’kis ma’mleketlik pedagogikali’q instituti’ rektori’ni’n’ <<_____>>_____2014-ji’l _____sanli’ buyri’g’i’ menen jaqlawg’a jiberilgen.

MAZMUNI’

Kirisiw

Civilizaciya rawajlani’wi’ni’n’ zamanago’y basqi’shi’nda informaciya tek g’ana ja’miyet ha’m ma’mleket ka’rxanalar iskerliginde, ba’lki ha’r bir insan turmi’si’nda ha’l yetiwshi ro’l woynaydi. Ko’z aldi’mi’zda ja’miyettin’ informaciyalasi’wi’ tez pa’t penen ha’m de ko’binese aldi’nnan bilip bolmaytug’i’n ta’rizde rawajlanbaqta. Biz bolsa tek ga’na woni’n’ social, ekonomikali’q, siyasiy ha’m basqa aqibetlerin tu’sinip jetiwge baslaymi’z. Ja’miyetimizdin’ informaciyalasi’wi’ jalg’i’z du’nya informaciya ma’kani’ni’n’ jarati’li’wi’na ali’p keledi de, bul ma’kan shen’berinde informaciyani’ jiynaw, qayta islew, saqlaw ha’m sub’ektler - insanlar, sho’lkemler, ma’mleketler wortasi’nda almasi’w a’melge asi’ri’ladi’.

Bizge belgili, siyasiy, ekonomikali’q, ilimiy-texnikali’q ha’m basqa informaciyalardi’ tezlik penen almasi’w imkaniyati’ ja’miyet turmi’si’ni’n’ barli’q tarawlari’nda ha’m a’sirese islep shig’ari’wda ha’m basqari’wda jan’a texnologiyalardi’n’ qollani’li’wi’ so’zsiz paydali’. Biraq sanaatti’n’ tezlikte rawajlani’wi’ Jer ekologiyasi’na qa’wip sala basladi’, yadro fizikasi’ tarawi’ndag’i’ jetiskenlikler yadro uri’si’ qa’wipin tuwdi’rdi’. Informaciyalasti’ri’w ha’m awi’r mashqalalar deregine aylani’wi’ mu’mkin.

Ha’r qanday uri’s, soni’n’ menen birge informaciya uri’si’, zamanago’y qural ja’rdeminde ali’p bari’ladi’. Informaciya qurali’ ja’rdeminde, uri’si’n ali’p bari’li’wshi’ ba’rshe qurallardan pari’qli’ ra’wishte, dag’aza qi’li’nbag’an ha’m ko’binese du’nyag’a ko’rinbeytug’i’n uri’slardi’ ali’p bari’w mu’mkin. Bul quraldi’n’ ta’sir ob’ektleri – ekonomikali’q, siyasiy, social ha’m t.b. kibi ja’miyet ha’m ma’mleket institutlari’. Mag’li’wmatlardi’ uzati’w tarmaqlari’ni’n’ keleshek jari’slar maydani’na aylani’wi’ a’lleqashan belgili bolg’an.

Internet XX a’srdin` en` joqari’ jetiskenligi esaplanadi’. Internet arqali’ pu`tkil dun`ya boylap jayi’li’p ketken neshe ju`z million komp`yuterlerdi ha`r biri ushi’n uli’wma bolg`an informaciyali’q wortali’qqa biriktiriw imkaniyati’ tuwi’ldi’.

Paydalani’wshi’ ko`z qarasi’nan global tarmaq birinshi na`wbette tarmaq abonentlerine wo`z-ara mag`li’wmatlar almasi’w, virtual tu`rde baylani’s jasaw imkaniyati’n jarati’p beriwshi "informaciyali’q magistral" wazi’ypasi’n atqaradi’, ekinshiden, wonda bar bolg`an mag`li’umatlar bazasi’ toplami’ dun`ya bilimler bazasi’n quraydi’. Soni’n` menen birge internet bu’gu’ngi ku`nde du’nya bazari’n u`yreniwde, marketing jumi’slari’n sho`lkemlestiriwde zamanago`y biznestin` en` a`hmiyetli qurallari’nan birine aylani’p qaldi’.

Internet to`mendegi imkaniyatlari’ menen belgili: informaciyag`a iye boli’w, jan`ali’qlar menen tani’si’w, bilimge iye boli’w, oqi’w, aldi’ng`i’ texnologiyalar ha’m ta`jiriybeler menen tani’si’w, jumi’s waqti’nda payda bolatug`i’n ma`selelerdi tezde sheshiw ha’m buyi’rtpashi’lardi’ baqlap bari’w h.t.b. Demek, internet -bul jan`ali’qlar menen u`zliksiz tu`rde tani’si’w, birgelikte islesiw ha’m ha`reketlerdin` birigiwi, zamanago`y pikirler almasi’w, bilimler menen almasi’w, ta`lim ali’w, isbilermenlik usi’li’ boli’p tabi’ladi’. Demek, internet - bul infra ortali’q boli’p, oni’n` ja`rdeminde mag`li’wmatlardi’ uzati’w, qabi’l qi’li’w, basqari’w ha’m shi’g`ari’w mumkin. Internet dun`ya ju`zinin` intellektual bayli’gi’na ha’m a`sirese aldi’ng`i’ texnologiya ha’m ta`jiriybelerge jol ashadi’, adamlar ha’m xali’qlar arasi’nda baylani’s ornatadi’.

Zamanago`y komp`yuter ha’m informaciyali’q texnologiyalardi’ ekonomika, ilim ha’m ta`limnin` barli’q tarawlari’na ken` engiziw, xali’qara informaciya sistemalari’na, soni’n` menen birge Internetke kirip bari’wi’n ken`eytiriw, joqari’ da`rejedegi programmistler tayarlaw jumi’slari’n jedellestiriw ma`selesi ma`mleketlik siyasat da`rejesine ko`terildi.

Internet – tarmaqlar ara informaciyalar almasi’wi’n ta`miynlewshi magistral` ekenligin ha`mmemiz jaqsi’ bilemiz. Internet ja`rdeminde dun`ya bilimler bazasi’na kiriw, qi’sqa waqi’t ishinde ko`plegen mag`li’wmatlardi’ ji’ynaw, islep shi’g`ari’w ha`m oni’n` texnikali’q qurallari’n arali’qtan turi’p basqari’w mumkin. Soni’n` menen bir qatarda internettin` bunday imkaniyatlari’nan paydalani’p tarmaqdagi’ biytani’s shaxs komp`yuterlerdi basqari’wi’, olardi’n`

mag`li'umatlar bazasi'na kiriw, nusxalaw, zi'yan keltiriw maqsetinde tu`rli viruslar tarqati'w kibi ni'zamg`a say bolmag`an ha`reketlerdi a`melge asi'ri'w mu'mkin.

Komp`yuterlerdi a`skeriy, kommerciyali'q, banklik, da`lda`lshilik, ilimiy izertlewdin` joqari' texnologiyali'q h.t.b tarawlari'nda qollani'wlari'n aji'rati'p atap o`tiwge boladi'. Informaciyani' jetkerip beriw ha`m qayta islew ushi'n komp`yuterlerdi ha`m komp`yuter tarmaqlari'n ken` qollani'w menen birge bul informaciya saqlani'p turg`an komp`yuterlerdi jat adamlardi'n` bularg`a kiriwinen isenimli tu`rde qorg`awi' kerek yekenligi ayday ayqi'n. Statistikali'q mag`li'wmatlar boyi'nsha 80% shamalas kompaniyalar wo`zlerinin` paydalani'p ati'rg`an mag`li'wmatlari'ni'n` pu`tinligi ha`m konfidencialli'g`i' (qupi'yali'g`i') buzi'li'w na`tiyjesinde finansli'q shi'g`i'nlarg`a ushramaqta.

Informaciyali'q ja'miyet jag'dayi'nda jaqsi' na`tiyjeler menen birgelikte bir qatar unamsi'z belgiler de bar. Mi'sali', komp`yuterlerdin' Internetke jalg'ang'anli'g'i' bir jag`i'nan du`n`ya ju`zinde toplang`an ko`p mug`dardag`i' paydali' informaciyadan millionlap adamlar paydalani'wina mu`mkinshilik berdi, al yekinshi ta'repten tarmaqta jaylasti'ri'lg`an ha`m wonda saqlani'p turg`an ha`r bir adamni'n` jeke aqi'l miynetin qorg`aw, wolardi'n' avtorli'q huquqi'n qorg'aw boyi'nsha mashqala payda yetedi.

Yesaplaw texnikasi'nda qa`wipsizlik tu`sinigi ken` mag`anag`a iye. Bul tu`sinikke komp`yuter jumi'si'ni'n` isenimliligi, mag`li'wmatlardi'n` saqlani'wi', informaciyani'n` ruxsatsi'z wo`zgerisler kiritiliwden qorg`ang`anli'g`i', elektron pochta xabarlari'ni'n` si'r saqlani'wi' h.t.b. kiredi. Barli'q rawajlang`an ma`mleketlerde informaciyani'n` pu`tinligi, konfidencialli'g`i' ni'zamli' tu`rde ta`miyinlenedi. Informaciyani' qorg`awdi'n` ha`r tu`rli jollari' bar, olardi'n` ishinde kriptografiyali'q usi'llar joqari' da`rejede qa`wipsizlikti ta`miyinleydi ha`m soni'n` menen birge paydalani'wshi'larg`a mag`li'wmatlardan paydalani'wda qi'yi'nshi'li'q tuwdi'rmaydi'.

Komp`yuter texnologiyalari'ni'n` informaciyani' qayta islew ha`m basqari'wdi' avtomatlasti'ri'w sistemalari'nda ken` qollani'li'wi' komp`yuter

sistemalari’nda aylani’p ju`rgen informaciyani’ ruxsat yetilmegen shaxslardan qorg`aw mashqalasi’n ju`zege keltirdi. Komp`yuter sistemalari’nda informaciyani’ qorg`aw bir qatar specifik qasiyetlerge iye, sebebi informaciya tasi’wshi’ menen qatan’ tu`rde baylani’sqan bolmay, an`sat nusqalanali’wi’ ha`m baylani’s kanallari’ arqali’ tarqati’li’wi’ mu`mkin.

Informaciyag`a qa`wip tek g`ana si’rttan yemes, ba`lki ishki paydalani’wshi’lar ta`repinen tuwdi’ri’li’wi’ mu`mkin. Informaciyali’q sistema bolg`an komp`yuter tarmaqlari’nda informaciyani’ qorg`aw apparatli’q ha`m programmali’q jaqtan ta`miyinleniwi mu`mkin. Ha`zirgi waqi’tlari’ ha`r qi’yli’ operaciyali’q sistemalar ushi’n arnalg`an qa`wipsizlik sharalar kompleksi islep shi’g`i’lg`an. Degen menen, xakerler ha`m bos oti’rg`ani’ joq, olar ha`r bir sistemani’n` ha`lsiz jerlerin tawi’p, ha`zil ushi’n yaki basqa bir maqsette paydalani’w ushi’n informaciyag`a ha`r tu`rli hu’jimler yetiwi mu`mkin. Sol sebepli, yag`ni’y payda bolg`an qa`wipsizlik mashqalalari’ sebepli hu’jim xarakterine qaray informaciyali’q sistemalardi’ qorg`awdi’n` jan`a sharalari’n islep shi’g`i’wdi’ talap yetedi.

Mashqalani’n’ aktualli’g’i’ talabalarg’a informaciya qa’wipsizligi haqqi’nda tu’sinik beriw ha’m woni’ qorg’aw jollari’n u’yretiw za’ru’rligin keltirip shi’g’aradi’. Magistrli’q dissertaciya talabalarg’a informaciya qa’wipsizligin ta’miyinlew jollari’n u’yretiw ma’selelerine bag’i’shlang’an.

I-BAP. İNFORMACIYA QA`WIPSIZLIGI TU`SINIGI

1.1. Informaciyali’q-kommunikaciyali’q sistemalarda informaciya qa`wipsizligi

Kommerciyali’q mekemelerde qa’wipsizlikti ta’miyinlew wo’zinin’ birinshi gezektegi wazi’ypasi’ yemes, ba’lki woni’ ta’miyinlewge sari’planatug’i’n qa’rejetlerdi uli’wma tiykarlanbag’an dep kelgen. Qandayda da’rejede bul "aqi’lli’ jumi’s": woni’si’z da jumi’s wori’nlawda tosi’qlar toli’p-tasi’p jati’r-g’o! Biraq firmani’n’ barli’q korporativ binalari’na keshe-ku’ndiz kiriwge ruxsat beriwge ju’rek yetiwshi aqi’li’ jayi’nda "sanaat kapitanlari’n" ko’rgenbisiz? A’lbette, joq! Ha’tte kishkene kompaniya binasi’ni’n’ kiriw joli’nda sizdi qarawi’l, yaki kiriwdi shegaralawshi’ ha’m nazarat yetiwshi sistemasi’ qarsi’ aladi’. Informaciyani’ qorg’aw bolsa yele ko’n’ildegidey yemes. Informaciyani’ qanday joq yetiw mu’mkinligin ha’m bul qanday aqi’betlerge ali’p keliwin barli’q adam tu’sine bermeydi.

U’lken woyi’nshi’lar jaqsi’ sabaq aldi’: xakerler Yahoo.com, Amazon.com kibi kompaniyalarg’a ha’m ha’tte kosmik izertlew agentligi NASAg’a u’lken zi’yan jetkizdi. Qa’wipsizlik xi’zmeti bazari’ni’n’ yen’ u’lkenlerinen biri RSA Security, ha’r qanday aqibetke qarsi’ shara barli’g’i’ haqqi’ndag’i’ woylamastan qi’lg’an bayanati’nan bir neshe ku’nnen keyin hu’jimge ali’ndi’[2-9].

A’dette adamlardan yaki predmetlerden shi’g’atug’i’n ha’m zi’yan jetkizetug’i’n qa’wipler to’mendegi klaslarg’a bo’linedi: *ishki* yaki si’rtqi’ *ha’m du’zilmelengen* (belgili ob’ektke qarsi’) yaki du’*zilmelenbegen*. Ma’selen, kompyuter viruslari’ "si’rtqi’ du’zilmelenbegen qa’wipler" si’pati’nda tu’rkimlenedi ha’m pu’tkil a’piwayi’ yesaplanadi’. Qi’zi’g’i’ sonda, paydalani’wshi’lar wo’zinin’ kompyuterin belgili nishan dep yesaplamaydi’, wolar wo’zlerin jaqsi’g’ana qorg’ang’anday sezedi. Kerekli qorg’aw da’rejesi ko’pshilik hallarda jumi’si’n’i’zdi’n’ jag’dayi’na baylani’sli’. Yeger mekemenin’ yaki kompaniyan’i’zdi’n’ qandaydi’r nishani’ bolsa, yeger siz milliy energetik resurslardi’ bo’listiriwshi yaki milliy baylani’s tarmaqlari’na xi’zmet qi’li’wshi’

ma’mleket infradu’zilisi qurami’nda bolsan’i’z, a’piwayi’ terroristlar bombalari’n ha’m pistoletlerin shetke qoyi’p, ha’r tu’rli da’stu’riy qurallar ja’rdeminde mekemen’izge elektron hu’jimdi a’melge as’i’ri’w ma’selesin ko’redi. Yekinshiden, sawda-sati’q ha’m marketing boyi’nsha a’piwayi’ mekeme tuwri’si’nda so’z barsa, tek klientler dizimin uri’lawshi’ xizmechilerin’iz tuwri’si’nda, wo’tirik kredit kartochkalari’ boyi’nsha tovar ali’wshi’ jinayaChi’lar, tarmag’i’n’i’zg’a preyskurantlardan paydalani’w maqsetinde kiriwshi qarsi’laslar, Web-saytin’i’zdi’ da’mego’yshilik maqsetinde buzi’wshi’lar ha’m sog’an uqsaslar tuwri’si’nda qayg’i’ri’wi’n’i’zg’a tuwra keledi.

Bizge belgili, du’nya informaciya ma’kani’na jalg’anbastan ma’mleket ekonomikasi’n rawajlandi’ri’p bolmaydi’. Internet tarmag’i’ ta’repinen ta’miyinlengen informaciya ha’m yesaplaw resurslari’nan operativ paydalani’wdi’ ma’mlekeChilikti, puxarali’q ja’miyet institutlari’n bekkemlew, social infradu’zilmelerinin’ rawajlani’w sha’rtleri si’pati’nda ko’riw mu’mkin.

O‘zbekistan Respublikasi’ni’n’ 1993-ji’l 7-maydag’i 848-XII-sanli «Ma’mleket si’rlari’n saqlaw tuwri’si’nda»g’i [3] ni’zami’ni’n’ 1-ba’ndinde ma’mleket si’rlari’ tu’sinigi berilgen:

> Ma’mleket ta’repinen qorg’alatug’i’n ha’m arnawli’ dizimler menen shegaralap qoyi’latug’i’n ayri’qsha a’hmiyetli, pu’tkil si’rli’ ha’m si’rli’ a’skeriy, siyasi’y, ekonomikali’q, ilimiy-texnikali’q ha’m basqa tu’r mag’li’wmatlar O‘zbekistan Respublikasi’ni’n’ ma’mleketlik si’rlari’ yesaplanadi’.

Usi’ ni’zamni’n’ 3-ba’ndinde ma’mleketlik si’rlardi’n’ taypalari’ keltirilgen: O‘zbekistan Respublikasi’ni’n’ ma’mleketlik si’rlari’ – ma’mleket, a’skeriy ha’m xi’zmet si’rlari’n qamti’p aladi’.

Informaciya qa’wipsizligi degende ta’biyiy yaki jasalma xarakterdegi tosi’nanli’ yaki qasttan qi’li’ng’an ta’sirlerden informaciya ha’m woni’ qollap-

quwwatlap turi’wshi’ infrastukturani’n’ qorg’alg’anli’g’i’ tu’siniledi. Bunday ta’sirler informaciya tarawi’ndag’i’ muna’sibetlerge, atap aytqanda, informaciya iyelerine, informaciyadan paydalani’wshi’larg’a ha’m informaciyani’ qorg’awdi’ qo‘llap quwwatlawshi’ infrastrukturag’a awi’r ziyan keltiriliwi mu’mkin.

O‘zbekistan Respublikasi’ni’n’ 2002-ji’l 12-dekabrdegi №439-II-sanli’ «Axborot erkinligi prinsiplari va kafolatlari to‘g‘risida»g’i’ ni’zami’nda [1,2] informaciya qa’wipsizligi informaciyani’n’ qa’wipsizligi dep belgilengen ha’m wol informaciya tarawi’nda shaxs, ja’miyet ha’m ma’mleket ma’plerinin’ qorg’alg’anli’q jag’dayi’n an’latadi’.

Ma’mleketein’ xali’qarali’q telekommunikaciya sistemasi’nda ha’m informaciya almasi’ni’wi’nda qatnasi’ni’n’ informaciya qa’wipsizligi mashqalasi’n kompleksli sheshpesten mu’mkin yemesligin ani’q ko’z aldi’mi’zg’a keltiriw qi’yi’n. A’sirese, jeke informaciya resurslari’n qorg’aw mashqalasi’ informaciya ha’m telekommunikaciya texnologiyalar tarawi’nda rawajlang’an ma’mleketlerden texnologiyali’q arqada qali’p ati’rg’an ma’mleketler ushi’n a’hmiyetli yesaplanadi’.

Informaciya qurali’n islep shi’g’i’wdi’ ha’m woni’ isletiwdi ximiyali’q ha’m bakteriologiyali’q qural kibi ani’qlaw itimalli’g’i’ uzaq. Da’l sol kibi ko’pshilik ma’mleketlerdin’ jalg’i’z global informaciya ma’kani’n qa’liplestiriw boyi’nsha uri’ni’wlari’n shegaralap bolmaydi’.

1.2. Informaciyali’q sistemalarg’a hu’jim tu’sinigi

Sistema administratori’ ushi’n qorg’awdi’n’ konkret da’rejesin ta’miyinlewdin’ jalg’i’z usi’li’ – informaciyag’a iye boli’wi’, sebebi ha’zirshe informaciya hu’jimine yen’ tez reakciya beretug’i’n insan yesaplanadi’. Demek, informaciyani’ qorg’aw administratorlari’ni’n’ woqi’ti’wg’a ha’m professional wo’siwine sari’p-qarejet informaciya hu’jimlerine qarsi’ turi’wshi’ yen’ na’tiyjeli qural yesaplanadi’.

Informaciyali'q sistemag'a hu'jim dep jawi'z shaxsti'n' informaciyali'q sistemani'n' ha'lsiz jerlerinen paydalani'p, maqsetli tu'rde informaciyadan ruxsatsi'z paydalani'wi', woni'n' pu'tinligi ha'm konfidencialli'g'i' buzi'li'wi'na ali'p keletug'i'n ha'reketler jiynag'i'na ayti'ladi'.

Agressiv bolmag`an ataka (hu'jim) - bul keyinshelik hu'jim qi'li'w maqsetinde aldi'nan ashi'q dereklerden ka`rxanani'n` tarmag`i' haqqi'nda informaciya ji'ynaw.

> Hu`jim (buzi'w, kiriw) – bul si'rli' informaciyani' ashi'w, sistemani'n` isenimliligin, turaqli'li'g`i'n to`menletiwge ali'p keletug`i'n belgili bir ha`reketler.

Agressiv bolmag`an hu'jimge mi'sallar:

- Informaciyali'q razvedka
- Portlardi' skanerlew
- Signaturalar tiykari'nda tu`yin (uzel) haqqi'nda informaciyani' qolg`a kiritiw
- Tarmaq ha`m tu`yinlerdi tabi'w

Informaciyali'q razvedka texnikasi'

Hu`jim qi'lmaqshi' bolg`an shaxslardi' qi'zi'qti'ratug`i'n tiykarg`i' informaciya:

- Sistemani'n` konfiguraciyasi'
- Ha`rekettegi paydalani'wshi'lardi' sistemag'a ali'w jazi'wlari'
- Kontaktlar ushi'n informaciya
- Ekstranet ha`m uzaqtan dostup ali'w serverleri
- Biznes-partnerlar, qosi'li'w ha`m birigiw haqqi'nda mag`li'wmat

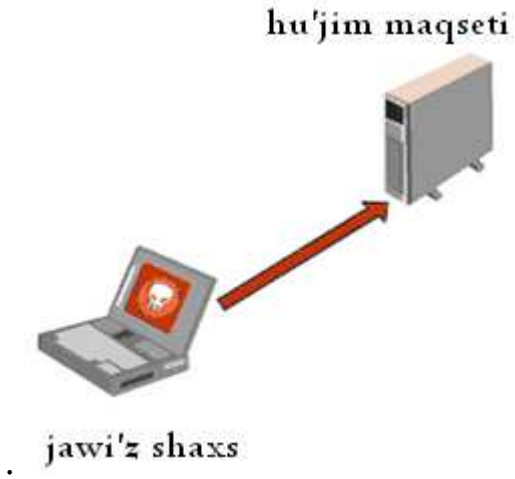
Tarmag`i’n`i’z haqqi’ndag`i’ informaciya to`mendegi dereklerden ali’ni’wi’ mu`mkin

- Kataloglarg`a zaproslar
- Korporativ web sayt
- Mag`li’wmat izlew mashinalari’
- Ashi’q forumlar

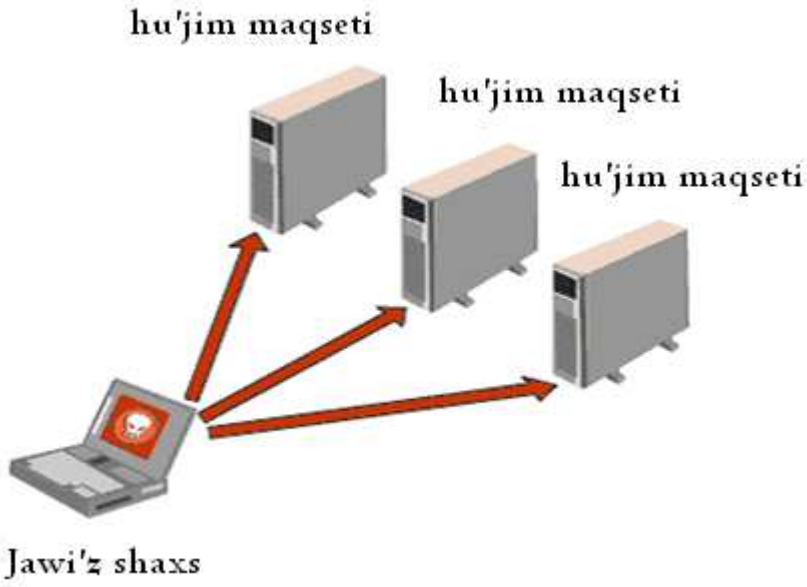
Demek, informaciyali’q sistemag`a hu’jim qa`wipin joq qi’li’w wondag`i’ kemshiliklerdi joq qi’li’w menen baylani’sli’. Bu`gingi ku`nde hu’jim tu`rlerinin` ani’q sani’ belgisiz. 1996 ji’l Fred Koen, virus texnologiyalari’ni’n` matematikali’q tiykarlari’n islep shi’g`i’p, wo`zinin` ilimiy izleniwleri na`tiyjesinde viruslar sani’ sheksiz degen pikirdi da`liyllegen. Bunnan komp`yuterlerge qi’li’natug`i’n hu’jimler sani’ da sheksiz degen pikir kelip shi’g`adi’, sebebi viruslar – bul hu’jimler ko`pliginin` u`les ko`pligi.

Hu`jim modelleri

Da`stu`riy hujim modeli «birge bir» (1-su’wret) yaki "ko`pke bir" (2-su’wret) principi tiykari’ndi’ quri’ladi’, yag`ni’y hujim bir derekten a`melge asi’ri’ladi’. Tarmaq qa`wpsizligin ta`myinlew sharalari’n islep shi’g`i’wshi’ ka`rxanalar (tarmaqlar ara yekranlar, hu’jimlerdi ani’qlawshi’ sistemalar h.t.b.) hu’jimlerdin` usi’ da`stu`riy modeline tiykarlanadi’. Qorg`ali’p ati’rg`an tarmaqti’n` ha`r qi’yli’ tochkalari’nda qa`wipsizlik agentleri (sensorlar) qoyi’ladi’, wolar informaciyani’ worayli’q basqari’w konsoline berip turadi’. Bul sistemani’ masshtablasti’ri’wdi’ an`satlasti’radi’ ha`m ali’stan basqari’wdi’ a`piwayi’lasti’radi’. Biraq bunday model` jaqi’nda ani’qlang`an (1998 ji’lda) hu’jim - bo`listirilgen hu’jimlerge qarsi’ kele almaydi’.

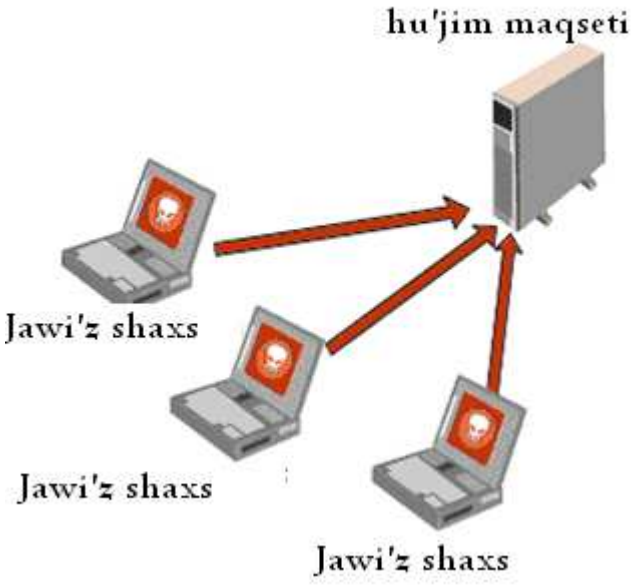


1-su’wuret . «Birge bir» hu’jimi

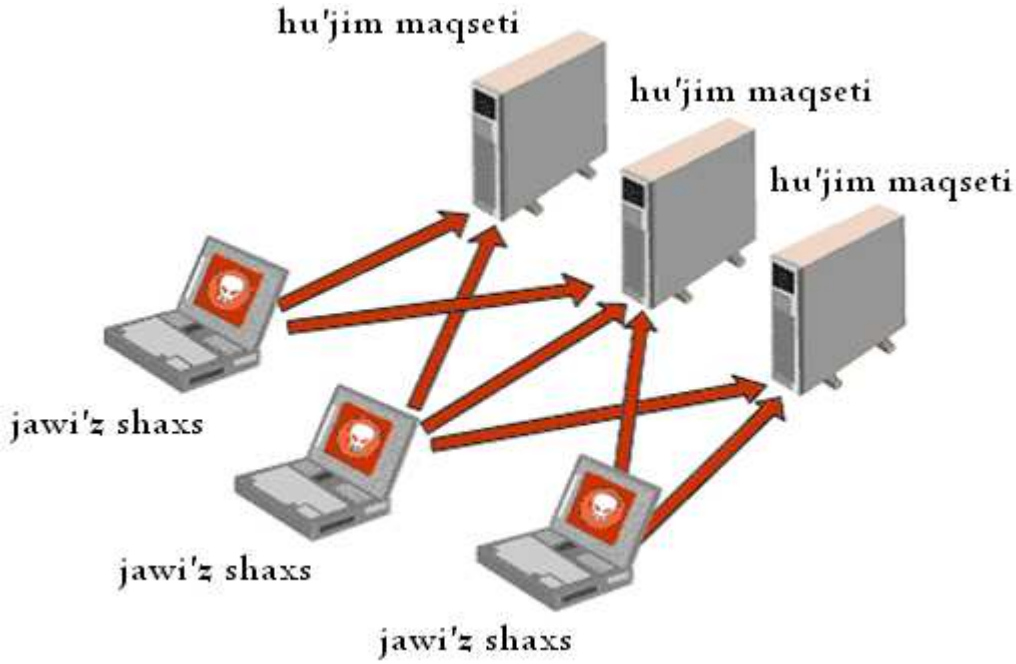


2-su’wret . «Ko`pge bir» hu’jim

Bo`listirilgen hu’jim modelinde basqa principlerden paydalani’ladi’. Da`stu`riy model`den pari’qi’ bul model`de «ko`pshilik boli’p birewge» , yaki «ko`plep birge» qatnasi’ (3-su’wret) ha`m "ko’pshilik boli’p ko`pshilikke", yaki «ko`plep ko`pke» qatnasi’ (4-su’wret) qollani’ladi’.



3-su’wret. "Ko`plep birewge" hu’jimi



4-su’wret. "Ko`pke ko`plep" hu’jim

Bunday hu’jimler sistemani’n` «xi’zmet ko`rsetiwge qarsi’li’q yetiw» hu’jim tu`rine jatadi’. Bunday hu’jimlerdin` ma`nisi hu’jim qi’li’ni’p ati’rg`an uzelge birdenine ko`p paket jiberiwden ibarat. Na`tiyjede uzel isten shi’g`i’wi’ mu`mkin, sebebi wol sonsha talaplardi’ birden wori’nlay almay qaladi’.

Hu'jimlerdi a`melge asi'ri'w basqi'shlari'

Hu'jimlerdi a`melge asi'ri'wdi'n` basqi'shlari' to`mendegishe:

1. hu'jimnen aldi'ng`i' ha`reketler, «informaciya ji'ynaw»
2. hu'jimdi a`melge asi'ri'w
3. hu'jimdi juwmaqlaw

A`dette hu'jim degende yekinshi basqi'sh tu`siniledi, biraq xaqi'yqati'nda hu'jimnin` birinshi ha`m u`shinshi basqi'shlari' u`lken a`hmiyetke iye. Informaciya ji'ynaw ha`m hu'jimdi juwmaqlaw, yag`ni'y izlerin joq qi'li'w wo`z gezeginde hu'jim dep ta`riypleniwi mumkin.

Informaciya ji'ynaw – bul hu'jimdi a`melge asi'ri'wdi'n` tiykarg`i' basqi'shi'. Tap usi' basqi'shtag`i' buzg`i'nshi'ni'n` is n`a`tiyjeliligi hu'jimnin` tabi'sli' juwmaqlani'w sha`rti boli'p tabi'ladi'. Da`slep hu'jim maqseti ani'qlanadi' ha`m wol haqqi'nda informaciya ji'ynaladi' (operacion sistema tu`ri, versiyasi', ashi'q portlar ha`m islep turg`an tarmaq servisi, wornati'lg`an sistemali' ha`m a`meliy programmali'q ta`miynlew ha`m woni'n` konfiguraciyasi' h.t.b.). Keyin buzg`i'nshi'ni'n` niyetin a`melge asi'ri'w mu`mkinshiligin beretug`i'n sistemani'n` yen` ha`lsiz jerleri identifikaciya yetiledi. Jaman niyetli shaxs hujim maqsetinin` basqa uzeller menen bolg`an barli'q baylani's kanallari'n ani'qlawg`a ha`reket yetedi. Soni'n` menen hu'jim tu`ri ha`m woni' a`melge asi'ri'w deregi ani'qlanadi'. Mi'sali', hu'jim qi'li'p ati'rg`an uzel yaki server menen islesip ati'r - OS Unix ha`m Windows NT serveri'. Bir server menen qatnasta isenim bar, al yekinshisi menen - joq. Jaman niyetli shaxs qaysi' server arqali' wo`zinin` maqsetin a`melge asi'ri'wi'na qarap, qaysi' hujim tu`ri qollani'wi', qanday a`melge asi'ri'li'wi' h.t.b. belgili boladi'. Sol informaciya tiykari'nda yen` jaqsi' effekt beretugi'n hu'jim a`melge asi'ri'ladi'.

1.3. Kompyuter viruslari’ informaciyali’q sistemalarg’a hu’jim tu’ri si’pati’nda

Kompyuter viruslari’ menen gu’resiw ju’da’ ah’miyetli ha’m quramali’ ma’sele, sebebi viruslar kompyuterlerdin’ normal islewin buzi’p g’ana qalmastan, ba’lkim wondag’i’ barli’q bar mag’li’wmatlardi’ buzi’wi’ ha’m ha’tte bul mag’li’wmatlardi’ joq yetiwi mu’mkinligi ja’nede qa’wipli. Kompyuterdin’ viruslar menen buzi’lg’an jumi’s qa’bileti’n virusqa qarsi’ programmalardi’ isletip barli’q waqi’tta tiklew mu’mkin, biraq joyti’lg’an mag’li’wmatlardi’ barli’q waqi’tta tiklew imkaniyati’ joq.

PC yadi’ndag’i’ mag’li’wmatlardi’, ba’zi’da uzaq waqi’t dawami’nda jarati’latug’i’n ha’m ji’ynalatug’i’n ah’miyetli informaciyani’ joyti’w yen’ awi’r jag’daylarg’a ali’p keliwi mu’mkin.

Viruslar haqqi’nda qi’sqa mag’li’wmat bereyik.

Kompyuter virusi’ — bul wonsha u’lken bolmag’an programma bo’li’p, wol g’a’rezsiz ra’wishte ko’beyiwi, wo’zin disklerge alı’p wo’tiwi, programmali’ fayllarg’a baylanı’sı’wi’, baylani’s kanallari’ ha’m kompyuter tarmaqlari’ bo’yi’nsha uzati’li’wi’ ha’m de ziyanlang’an disklerde unamsi’z ha’reketler wori’nlawi’ mu’mkin.

Bul maydalap du’zilgen ha’m ko’binese ju’da’ qa’wipli programma. Ba’zi’ bir viruslar ju’da’ xoshso’zli, ma’selen, a’piwayi’ bayram menen qutli’qlap ha’m ha’r qi’yli’ dawi’sli’ ha’m videoeffektlerdi jarati’wshi’, lekin sistemani’ toli’q isten shi’g’ari’wshi’ ha’m wondag’i’ mag’li’wmatlardi’ buzi’wshi’ jawi’z viruslar da bar.

Virus wo’zi jaylasqan programma menen ju’klenedi ha’m iske tu’sedi. Virus wo’zinin’ jawi’z niyetin a’melge asi’ri’wdan aldi’n tayarlanadi’:

Kompyuter virusi’ wo’zin yadti’n’ basqa jerine jazadi’, operaciyali’q sistemani’ modifikaciyalaydi’ (wo’zgertedi), ba’zi’da wo’zine, wo’zinin’ payda boli’wi’ deregin jasi’ri’w ushi’n, «si’rttan bilinbeytug’i’n ha’m inkubaciya da’wirin» sho’lkemlestiredi, basqa programmalarg’a a’meliy asi’p wo’tedi.

Virus programmalarg’a, operaciyali’q sistema, tarmaqli’ drayverler, magnit disklerdin’ sistemali’ oblasti’na ha’m t.b. Payda yetilgen bo’li’wi’ mu’mkin. Son’g’i’ waqi’tta tekstli fayllarg’a jug’i’wshi’, wolardi’ buzi’wshi’, wolardi’n’ wo’lshemlerin ko’p ma’rte artti’ri’wshi’ viruslar payda bo’ldi’.

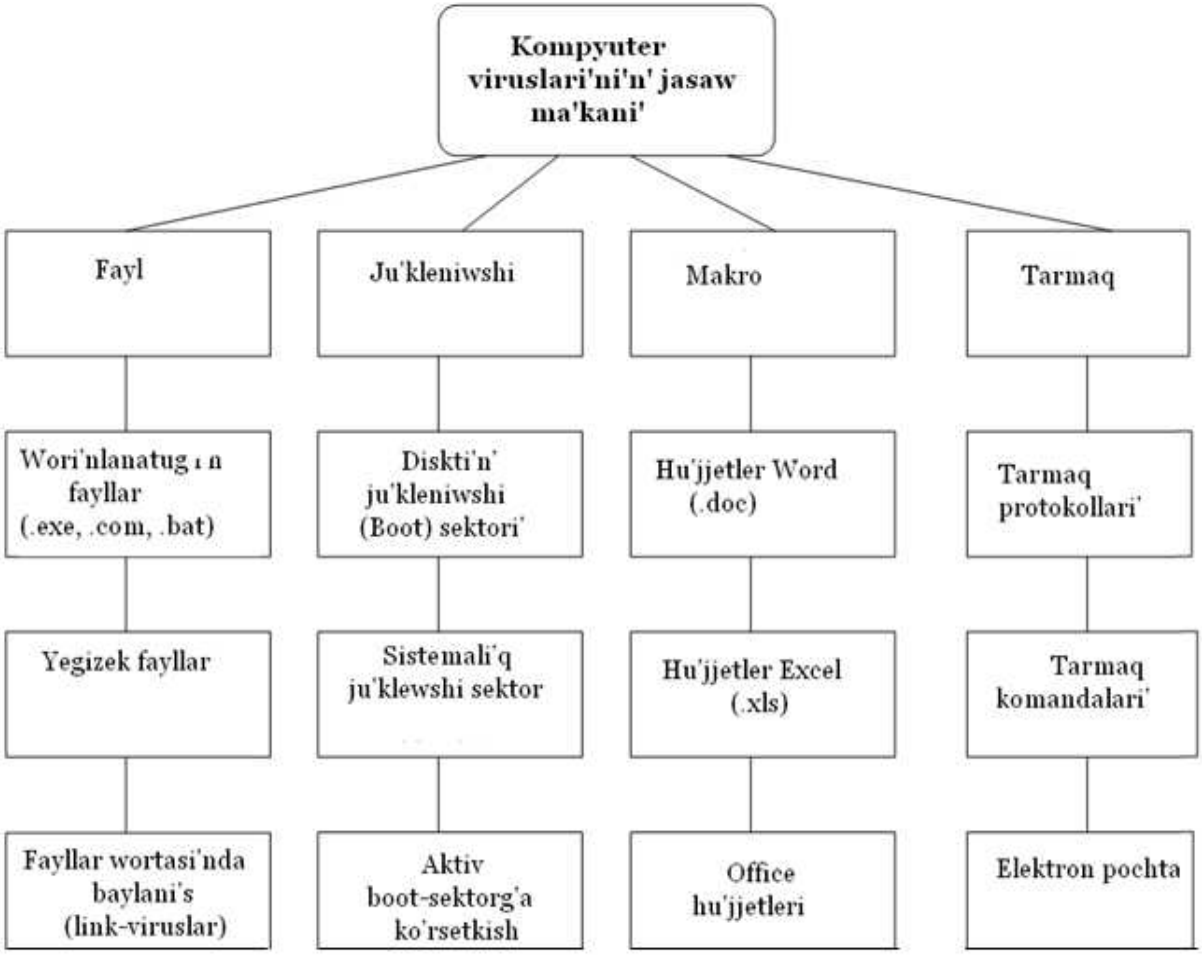
Viruslar aktivliginin’ yen’ ko’p ushi’raytug’i’n aqı’betleri

- operatsion sistemanı’ ju’klewdin’ imkanı joqlı’g’ı’;
- ma’islerdi nolge ten’glestiriw ha’m qa’legen wo’zgertiw;
- faylli’ sistemanı’ buzı’w (fayllardı’ aralastı’rı’p jiberiw, fayllar jaylası’w tablicası’n buzı’w);
- fayl wo’lshemlerin ko'beytip jiberiw;
- displey islewin buzı’w ha’m sog’an uqsas.

Yen’ birinshi ma’rte kompyuterlerdin’ viruslar menen ziyanlaniwi’ 15 ji’l aldi’n a’melge asi’ri’lg’an. 1987 ji’lda pakistanli’ programmistler Pakistanni’n’ programma wo’nimlerin arzan licenziyasi’z nusqalari’n sati’p alg’an amerikali’lardi’ jazalawg’a qarar qi’ldi’. Ni’zamsi’z sati’li’p ati’rg’an nusqalarg’a «pakistansha» virus (keyninen sonday dep atalg’an) tarqati’lg’an, wol AQSH ta 18 mi’n’nan arti’q kompyuterdi tez ziyanladi’ ha’m jer shari’ bo’ylap sayaxat qi’li’p,

jetip keldi. Keyin viruslar ha’m wolar menen ziyanlang’an kompyuterler sani’ tez ko’beye basladi’ ha’m ha’zir ken’ ma’lim bo’lg’an g’alaba viruslardi’n’ bir neshe won mi’n’i’ bar.

Kompyuter viruslari’ni’n’ tu’rleri ha’m wolardi’n’ wazi’ypalari’



1.4. Web te informaciyag’a qa’wip tu’rleri

Belgili bir web tu`yini yaki dun`ya ju`zlik tor xaqqi’nda maksimal da`rejede toli’q informaciya toplaw jollari’na bag`i’shlang`an a`debiyatlar Internet tarmag`i’nda jetkilikli. Tez-tezden ushi’rap turatug`i’n Web tori’ndag`i’ urli’q jag`daylari’ ha`m soni’n` qatari’nda boli’p maqseti bir boli’p tabi’ladi’.

Informaciyani’ qolg`a kiritiw maqsetinde buzg`i’nshi’lar qoldan barli’q Web-betliklerdi ko`zden wo`tiredi ha`m kodlarda, betliklerge berilgen kommentariylerde, web betliktin` dizayni’nda, strukturasi’nda ushi’raytugi’n kemshiliklerdi tabi’wg`a ha`reket yetedi.

To`mende Web-server xaqqi’nda informaciya ji’ynawdi’n` sonday jollari’nan bir neshe tu`ri keltirilgen. Bunday metodlarg`a betliklerdi izbe-iz ha`m birme-bir qoldan ko`rip shi’g`i’w menen birge bul procesti avtomatlasti’ri’w scenariylerinen ha`m kommerciyali’q programmalardan paydalani’w jollari’ ta`riyplengen.

Web betliklerdi birme-bir ko`rip shi’g`i’w. Mag`li’wmatlardi’ qolg`a kiritiwdin` yen` belgili bolg`an jollari’ni’n` biri boli’p Web-tu`yindi toli’g`i’ menen qoldan birme-bir ko`zden o`tiriw ha`m brouzerde ha`r bir betliktin` tiykarg`i’ kodlari’n tabi’w boli’p tabi’ladi’. HTML tilinde jazi’lg`an gipertekstli hujjetlerden ko`pshilik mag`li’wmatlardi’ tabi’w mu`mkin. Mi’sali’, basqa web dizayner-programmistler ushi’n jazi’lg`an a`hmiyetli kommentariyler, elektron pochta adresleri, kerekli telefonlardi’n` nomerleri, JavaScript programmasi’nda jarati’lg`an kishi programmalardi’n` listingi ha`m basqalar. Programmani’n` tiykarg`i’ kodi’ ko`p a`hmiyetli informaciyani’ o`z ishinde qamti’wi’ mu`mkin. Mi’sali’, kataloglar strukturasi’, web sayt avtori’ni’n` ati’, adresi, elektron pochtasi’ h.t.b.

Komanda: brouzerde i’qti’yari’y serverdin` adresi kiritilip, View^Page Source komandasi’ beriledi. Na`tiyjede ekranda web betliktin` tiykarg`i’ HTML kodi’ payda boladi’.

U`lken (30 betlikten aslam bolg`an) Web-tu`yinlerge ko`pshilik buzg`i’nshi’lar avtomatlasti’ri’lg`an joldi’ qollanadi’. Bunda arnawli’ scenariylerden yaki utilitalardan paydalani’ladi’. Bunday scenariylerdi ha`r qi’yli’ programmalasti’ri’w tillerde jazi’w mu`mkin. Ko`binese wolar Perl algoritmlik tilinde jarati’ladi’. Bul tilde jazi’lg`an wonsha quramali’ bolmag`an programmalar ja`rdeminde Web-server boyi’nsha sayaxat yetiw ha`m belgili gilt so`zler ja`rdeminde qalegenshe kerekli mag`li’wmatlardi’ izlep tabi’wg`a boladi’.

Bunday jol menen tabi'lg`an mag`li'wmatlardi' nusqalaw ushi'n ha`tteki bir neshe kommerciyali'q programma islep shi'g`i'lg`an boli'p, olar ha`r qi'yli' operaciyali'k sistemalar, mi'sali', UNIX, NT ushi'n mo`lsherlengen. Wolardi'n` ishinde yen` ken` tani'qli'si' NT operaciyali'q sistemasi' ushi'n arnalg`an Teleport Pro utilitasi' boli'p tabi'ladi'. Bul utilita Tennyson Maxwell Information Systems (http://www.tenmax.com) kompaniyasi' ta`repinen islep shi'g`i'lg`an. Programma lokal komp`yuterde toli'g`i' menen bir Web-tu`yindi ko`rsetiw ha`m woni'n` mazmuni' menen tani'si'p shi'g`i'w mu`mkinshiligin beredi.

Giltli so`zler boyi'nsha izlep tabi'w kriteriyine juwap beretug`i'n fayllardi' ju`klew ha`m olardi' analiz qi'li'w ushi'n olardi' lokal tu`rde ju`klew jetkilikli boladi'. Mi'sali', yegerde belgili bir gilt so`zlerdi o`zine qamti'ytug`i'n Web betliklerdi tabi'w kerek bolsa (wolar tiykarg`i' HTML kodlarda jaylasqan bolsa-da), mi'sali' email, contact, user*, pass*, updated h.t.b., bunday xi'zmetti Teleport Pro utilitasi' tabi'sli' a`melge asi'radi'. Bunda bul so`zlerdin` qalegen birewi boyi'nsha mag`li'wmatlardi' izlew tek g`ana belgili formatdag`i' fayllarda ali'p bari'ladi', mi'sali', *.htm. *.html, *.shtm, *.shtml, *.txt. '.cfm h.t.b. Bul programma izlep tabi'w kerek bolg`an so`zlerdi beriw mu`mkinshiligin ha`m ta`miynleydi.

Kerekli Web-betlikler lokal komp`yuterge nusqalani'p bolg`annan keyin, buzg`i'nshi' shaxs wolardi' izertlewge kirisiwi mu`mkin. Wol har bir gipertekstli HTML betligin, har bir grafikali'k fayl, basqari'w panelin ha`mde ishki du`zilistegi scenariylerdi u`yrenip shi'g`i'wi' mu`mkin ha`m sonday yetip, izertlenip ati'rg`an Web tu`yinnin` arxitekturasi'n tu`sinip ali'wg`a hareket yetedi. Bunday mag`li'wmatlardan keyinshelik buzg`i'nshi' wo`zinin` maqsetlerin a`melge asi'ri'w ushi'n tabi'sli' paydalani'wi' mu`mkin.

I BAP BOYINSHA JUWMAQ

Bul bapta informaciya qa`wipsizligi tu`sinigi, informaciyali'q-kommunikaciyali'q sistemalarda informaciya qa`wipsizligi haqqinda aytilg`an bolip, bunda kommerciyali'q mekemelerde qa'wipsizlikti ta'miyinlew, wo'zinin' birinshi gezektegi wazi'ypasi', adamlardan yaki predmetlerden shi'g'atug'i'n ha'm zi'yan jetkizetug'i'n qa'wipler, wolardin' tu'rleri, ta'biyiy yaki jasalma harakterdegi tosi'nanli' yaki qastan qi'li'ng'an ta'sirlerden informaciya ha'm woni' qollap-quwwatlap turi'wshi' infrastukturani'n' qorg'alg'anli'g'i' haqqinda aytiladi.

Informaciyali'q sistemalarg'a hu'jim tu'sinigi, sistema administratori' ushi'n qorg'awdi'n' konkret da'rejesin ta'miyinlewdin' usi'li', agressiv bolmag`an hu'jim, hu`jim qi'lmaqshi' bolg`an shaxslardi' qi'zi'qti'ratug`i'n tiykarg`i' informaciya, hu`jim modelleri, hu'jimlerdi a`melge asi'ri'w basqi'shlari' haqqinda so'z yetiledi.

Kompyuter viruslari', informaciyali'q sistemalarg'a hu'jim tu'ri, viruslar haqqi'nda qi'sqa mag'li'wmatlar ha'm wolardi'n' wazi'ypalari', viruslar aktivliginin' yen' ko'p ushraytug'in aqibetleri, web te informaciyag'a qa'wip tu'rler, belgili bir web tu`yini yaki dun`ya ju`zlik tor haqqi'nda maksimal da`rejede toli'q informaciya toplaw jollari', tez-tezden ushi'rap turatug`i'n web tori'ndag`i' urli'q jag`daylari' haqqinda mag'lwmatlar keltirilgen.

II-BAP. INFORMACIYALI’Q-KOMMUNIKACIYALI’Q SISTEMALARDA INFORMACIYANI’ QORG’AW JOLLARI’

2.1. Informaciya qa’wipsizligin ta’miyinlewdin’ apparatli’q-programmali’q qurallari’

Kompyuter sistemalari’ni’n’ quri’lmalari’nan paydalani’wg’a ruxsatti’ ali’stan turi’p basqari’w da mu’mkin. Mi’sali’, lokal tarmaqlarda isshi stanciyani’n’ tarmaqqa jalg’ani’wi’ administrator jumi’s worni’nan turi’p blokirovka qi’li’ni’wi’ mu’mkin. Quri’lmalardan paydalani’wg’a ruxsat yeti’wdi tok dereklerin u’zip qoyi’w arqali’ ha’m na’tiyjeli basqari’w mu’mkin. Bunda jumi’stan basqa waqi’tlarda, tok deregin qo‘rg’aw xi’zmeti ta’repinen baqlani’p bari’latug’i’n kommutaciyali’ quri’lmalar ja’rdeminde u’zip qoyi’ladi’.

Informaciyani’ qorg’awdi’n’ **tiykarg’i’ apparatli’q qurallari’na** to’mendegilerdi kiritiw mu’mkin:

– paydalani’wshi’ni’ identifikaciyalawshi’ mag’li’wmatlardi’ kiritiw quri’lmalari’ (magnit ha’m plastik kartalar, barmaq izleri h’am basqalar);

– mag’li’wmatlardi’ shifrlawshi’ quri’lmalar;

– jumi’s stanciyalari’ ha’m serverlerge ni’zamsi’z jalg’ani’p ali’wg’a ruxsat bermew quri’lmalari’ (elektron quli’plar ha’m blokiratorlar).

Mag’li’wmatlardi’ qorg’awdi’n’ **ja’rdemshi apparatli’q qurallari’na** to’mendegiler mi’sal bola aladi’:

– magnitli tasi’wshilardag’i’ ma’g’li’wmatlardi’ joq qi’li’wshi quri’lmalar;

– kompyuter quri’lmalari’nan paydalani’wdi’n’ ni’zamsi’z ha’reketleri boyi’nsha xabardar qi’li’wshi’ (signalizaciyani’ iske tu’siriwshi) quri’lmalar ha’m basqalar.

Informaciyalardi’ qorg’awdi’n’ tiykarg’i’ ***programmali’q qurallari’na*** to’mendegilerdi kiritiw mu’mkin:

– kompyuter sistemalari’nda paydalani’wshi’lardi’ identifikaciyalawshi’ ha’m autentifikaciyalawshi’ da’stu’rler;

– kompyuter sistemalari’ni’n’ resurslari’nan paydalani’wshi’lardi’n’ huquqlari’n sheklewshi da’stu’rler;

– informaciyalardi’ shifrlawshi’ da’stu’rler;

– informaciyali’q resurslardi’ (sistemali’ ha’m a’meliy da’stu’riy ta’miyinleniwdi, mag’li’wmatlar bazalari’n, ta’limnin’ kompyuter sistemalari’n ha’m t.b.) ni’zamsi’z wo‘zgertiriwlerden, paydalani’wlardan ha’m ko‘beytiriwlerden qorg’awshi’ da’stu’rler.

Qorg’awshi’ apparatli’-da’stu’riy komplekslerdin’ ko‘pshiliginde maksimal sandag’i qorg’aw mexanizmlerinen paydalani’ladi’. Bul mexanizmlerge to’mendegiler kiredi:

– paydalani’wshi’lardi’ identifikaciyalaw ha’m autentifikaciyalaw;

– fayllar, papkalar, disklardan paydalani’wda ruxsatti’ sheklep qoyi’w;

– da’stu’riy qurallar ha’m informaciya pu’tinligini baqlap bari’w;

– paydalani’wshi’ ushi’n funkcional jabi’q wortali’qti’ jarati’w imkaniyati’;

– OSti’n’ ju’kleniw procesin qorg’aw;

– paydalani’wshi’ joqli’g’i’nda kompyuterdi blokirovka qi’li’w;

– mag’li’wmatlardi’ kriptografiyali’q wo‘zgertiw;

– bolg’an hadiyselerdi registraciya yetip bari’w;

– kompyuter yadi’n tazalaw.

A`lbette, ayri’m jag`daylarda qa`wipsizlikti ta`miynlew ushi’n belgili bir sharalar ko`riw mu`mkin, biraq, ko`pshilik jag`dayda qa`wipsizlik sistemasi’ndag`i’ kemshiliklerdi saplasti’ri’w ushi’n arnawli’ ha`m sapali’ programmalar kerek boladi’. Bunday programmalardi’n` qatan’ logikasi’ ha`m mag`li’wmatlar ag`i’mi’n basqari’w mu`mkinshilikleri ku`shli boli’wi’ kerek. Soni’n` menen birge bunday sharalardi’n` barli’g`i’ ku`ndelik sistemalardi’n` monitoringi menen birge ali’p bari’li’wi’ kerek. Bunday monitoring bolsa ko`p ku`sh, di’qqat ha`m qunt talap yetedi.

Pu’tinlikti ta’miyinlew degende informaciyani ruxsatsi’z wo‘zgertirip bolmawi’na kepillik tu’siniledi. Pu’tinlikti kepillew ushi’n mag’li’wmatlar boyi’nsha belgili bir wo‘zgerti’ri’wlerdi a’melge asi’ri’wdi’ ani’qlaytug’i’n

a’piwayi’ ha’m isenimli norma boli’wi’ kerek. Bul wo‘zgertiriwler tekstti wo‘shiriw, almasti’ri’w, tazasi’n qoyi’w arqali’ a’melge asi’ri’li’wi’ mu’mkin.

Autentifikaciyalawdi’ ta’miyinlew informaciyali’q wo‘z ara muna’sibet procesinde informaciyani’n’ wo‘zin ha’m ta’replerdin’ haqi’qi’yli’g’i’n tasti’yi’qlaw usi’llari’n islep shig’i’wdi an’latadi’. Baylani’s kanali’ arqali’ uzati’latug’i’n informaciya deregi, jarati’lg’an sa’nesi, sho’lkemlestiriwshi mag’li’wmatlari’, uzati’w sa’nesi ha’m sol kibiler menen autenfikaciya qi’li’ni’wi’ kerek.

Avtorli’qti’ inkar yete almasi’g’i’n ta’miyinlew - bul subyektler ta’repinen a’melge asi’ri’lg’an ha’reketlerdi ta’n almasli’q jag’dayi’ mu’mkinliginin’ aldi’n aladi’.

Parollerdi qolg`a kiritiw mumkinshiligin beretug`i’n programmadan mag`li’wmatlardi’ qorg`aw. Informaciya qa`wipsizligin ta`miynlewde mag`li’wmatlardi’n` konfidencialli’g`i’n saqlaw – bul ju`da’ a`hmiyetli ma`sele. Bul tikkeley paydalani’wshi’ni’n` sistemag`a kiriw ushi’n bekitilgen paroline tiyisli. Parollerdi qolg`a kiritiw ushi’n buzg`i’nshi’lar nelerdi islemeydi, qanday jollardan paydalanbaydi’! Bunday nietlerdi a`melge asi’ri’wshi’ programmalar sol qatarg`a kiredi. Wolardi’n` ishinde usi’ni’latug`i’n xi’zmetleri (mu’mkinshilikleri) boyi’nsha xaqi’yqatdan da ku`shli programmalar paketi SnifferPro (wol ju`da’ qi’mbat!) yaki arzanraq qurallar, mi’sali’, CaptureNet programmasi’nan paydalani’wg`a boladi’. Bul programma Lavrentiy Nikula ta`repinen islep shi’g`i’lg`an. Biraq, yen` jaqsi’si’, Dag Song islep shi’qqan programmadan paydalani’w. Wol parollerdi uslap ali’p qolg`a kiritiwdin` yen` quramali’ qurali’n jaratqan, bul qural dsniff programmasi’ boli’p tabi’ladi’

Parol si’pati’nda shifrlanbag`an tekstti paydalani’latug`i’n qosi’mshalar jiyi’ ushi’rasadi’. Soni’n` menen birge bunday konfidencial informaciya jaqsi’ saqlanbaytug`i’nli’g`i’n da ayti’p o`teyik. Bunday qosi’mshalarg`a mi’sal etip NNTP, ICQ, IRC, Socks, NFS (tarmaqti’n` faylli’q sistemasi’— Network File System), mountd, rlogin, IMAP, AIM, XI1, CVS, Napster, Citrix ICA, pcAnywhere, NAI Sniffer, Microsoft SMB ha`m Oracle SQL keltiriw mumkin.

Keltirilgen qosi’mshalardi’n` ko`pshiliginde shifrlanbag`an tu`rde paydalani’wshi’lardi’n` atlari’ ha`m parolleri, yaki wolardi’ shifrlawda, jasi’ri’w ha`m dekodirovanie qi’li’wda a`piwayi’ algoritmler qollani’lg`an boladi’. Ta`biyiy, wolar buzg`i’nshi’ ushi’n tosi’q bola almaydi’. Tap usi’nday jag`dayda dsniff programmasi’ni’n` ku`sh-qudiretin toli’q seziwge boladi’.

2.2. Jeke kompyuterlerde informaciya qa’wipsizligin ta’miyinlew jollari’

Ha’r bir paydalani’wshi’ni’n’ jeke kompyuterinde de informaciya qa’wipsizligi siyasati’n ali’p bari’w kerek. Viruslar menen gu’resiw ushi’n qanday usi’ldi’ qollani’w mu’mkin?

• yen’ da’slep *«keselliktin’ aldi’n ali’w usi’llari’»* — PC di viruslar kirip keliwinen qorg’aw. Buni’n’ ushi’n:

• kompyuterge kelip shi’g’i’wi’ gu’manli’ programmalardi’ wo’rnatpaw kerek *(programmalardi’ ta’rtipsiz ko’shirip jazi’wdan saqlani’n’), y*eger buni’n’ ilaji’ bo’lmasa, jan’a programmalardi’ wo’rnati’wdan aldi’n woni’ a’lbette virusqa qarsi’ qurallar menen tekserin’;

• wo’zin’nin’ fleshkan’i’zdi’ basqa kompyuterde isletkende jazi’wdan barli’q waqi’tta saqlan, basqa fleshkani’ wo’zin’izdin’ kompyuterin’izde isletkende bolsa woni’ a’lbette aldi’nnan viruslarg’a qarsi’ qurallar menen tekserin’;

• telekommunikaciya sistemalari’ menen ha’m tarmaqdar menen kompyuter islegende baylani’s kanaldan kiriwde virusqa qarsi’ filtrler qo’yi’n’ (ha’zir sondaylarda payda bo’ldi’).

Jeke kompyuterdi viruslardin’ destruktiv ta’sirinen qorg’aw, qaytari’p bo’lmaytug’i’n buzuli’wlardi’ ha’m ma’nislerdi joyi’ti’wdi’ saplasti’ri’w ushi’n:

• mag’li’wmatlardi’ si’rtqi’ tasi’wshi’larg’a jazi’w bo’yi’nsha mu’rajat yetiwden qorg’aw;

• disklerdin’ sistemali’ oblasti’n ha’m kerekli fayllardi’ basqa ko’rinistegi tasi’wshi’larg’a nusqasi’n ali’p qo’yi’n’;

• fayllardi’ ayi’ri’m bo’leklerge aji’rati’wdi’ barqulla wori’nlaw kerek, sebebi bul programma wori’nlani’wi’n tezlestirip g’ana qalmastan, ba’lkim programmalar buzi’lg’anda wolardi’ tiklewdi de jen’illestiredi.

Son’i’nda, kompyuterge kirip alg’an viruslardi’ tabi’w ha’m biyta’rep yetip qo’yi’w. Bul processler arnawli’ virusqa qarsi’ programma quri’lmalari’n isletiw menen a’melge asi’ri’ladi’:

• viruslardi’ si’rtqi’ infomaciya tasi’wshi’larda da, kompyuter yadi’nda da izlew ha’m tabi’wdi’ a’melge asi’ri’wshi’ programma — *qadag’alawshi’ (detektor);*

• viruslardi’ wolar jaylasqan wortali’qta tiklep, ha’m tiklemesten joq qi’li’wdi’ wori’nlawshi’ deinfektorlar (doktorlar, faglar — yad bo’leksheler ha’m bakteriyalardi’ juti’wshi’ ha’m si’n’i’ri’wshi’ «kletka»);

• viruslar ushi’n sa’ykes bo’lg’an ha’reketlerdi ani’qlaytug’i’n ha’m paydalani’wshi’dan wolardi’ wori’nlawdi’n’ ni’zamli’li’g’i’n tasti’yi’qlawdi’ talap yetetug’i’n programma — *filterler (qarawi’llar);*

• ani’q viruslardi’ jasaw wortali’g’i’n ha’m yadta jug’i’wi’n saplasti’ri’wshi’ ha’m soni’n’ menen wolardi’n’ ko’beyiw qa’bileti’n bloklawshi’ *programma-immunizatorlar* — virus juqti’rmaytug’i’nlar *(yemlegishler).*

Ha’zirgi waqi’tta joqari’da ko’rsetilgen wazi’ypalardi’ birge qosi’p wori’nlaytug’i’n ko’pshilik virusqa qarsi’ programmali’ qurallar ha’m virusqa qarsi’ programmali’ sistemalar islep shi’g’i’lg’an. To’medegi sistemalar yen’ ko’p qo’llani’lmaqta:

• virusga qarsi’ Doctor Web sistemasi’, wol mi’n’lap ma’lim viruslardi’ bayqaydi’ ha’m joq qi’ladi’, sazlang’an processor ha’m evristik analiz blogi’ni’n’ barli’g’i’ yesabi’na bolsa ko’plep belgisiz viruslardi’ da bayqaydi’;

Soni’ ayti’p wo’tiw kerek, ha’mme ayti’p wo’tilgen virusqa qarsi’ qurallardi’ islep shi’g’ari’wshi’lar jan’a viruslari’n’ payda bo’li’wi’n di’qqat penen baqlap baradi’ ha’m wolar menen gu’resiw qurallari’n tez tayarlaydi’. Bul barli’q viruslarg’a qarsi’ qurallardi’n’ versiyalari’n ani’qlaw ha’r ayda a’melge asi’ri’ladi’. Licenziyali’ virusqa qarsi’ programmani’ sati’p ali’p, woni’n’ keleshektegi barli’q

modifikaciyalari’na abonent bo’li’w mu’mkin ha’m a’dette, wolardi’ biypul yaki arzi’mag’an bahalarda ali’w mu’mkin.

Soni’n’ ushi’n yen’ birinshi wazi’ypa: kerekli informaciyali’ barli’q fayllardi’ kompyuterlerden avtonom bo’lgan infomaciya tasi’wshi’larda: fleshkalarg’a, ali’natug’i’n qatti’ disklerde, CD- ha’m DVD-RAM larda, magnit lentalarda ha’m basqalarda a’lbette nusqasi’n ali’p qo’yi’n’ (bul wazi’ypa viruslarsi’z da aktual).

2.3 Informaciyali’q sistemalarda informaciya qa’wipsizligi siyasati’n a’melge asi’ri’w

Ka`rxanalardi’n` informaciyali’q qa`wipsizlik si’yasati’ ti’ni’msi’z tu`rde informaciyali’q qa`wipsizlikti analiz qi’li’w ha`m payda bolg`an qa`wiplerge tezde qarsi’ sharalar islep shi’g`i’wg`a tiykarlang`an boli’wi’ kerek. Qa`wipsizlik analizi’ bunda bas rol` woynaydi’ ha`m to`mendegi sorawlarg`a juwap ali’wdi’ na`zerde tutadi’.

Ne ushi’n tarmaqlardi’ buzi’w ha`reketleri a`melge asi’ri’ladi’?

- Adam faktori’ (juwapkersizlik)
- Uli’wma siyasatti’n` buzi’li’wi’, buyri’qlardi’n` wori’nlanbawi’
- Programmali’q ha`m apparatli’q ta`miynleniwdin` qa`te sazlang`anli’g`i’
- Tarmaqti’ toli’g`i’ menen u`yrenip shi’qpag`anli’q
- Kompetentligi to`men paydalani’wshi’lar kesirinen
- Programmali’q ta`miynleniw wo`z waqti’nda jan`alani’p turmag`anli’g`i’

***Informaciyali’q sistemani’n` qa`wipsizlik jag`dayi’n analiz qi’li’w.*** Informaciyani’n` qorg`ang`anli’g`i’n analiz qi’li’wda to`mendegi sorawlarg`a juwap beriw kerek:

- Tarmag`i’mi’z qorg`alg`an ba? Woni’ qalay bilemiz?
- Qa`wipsizlikti ta`miynlewdi jaqsi’law boyi’nsha usi’ni’slardi’ tayarlap qoyi’w

- Nastroykadag`i’ qa`telerdi tabi’w ha`m qa`wipsizlik sharalari’n jan`alap turi’wdi’ sho`lkemlestiriw
- Ka`rxanani’n` qa`wipsizlik sistemasi’ndag`i’ ku`tilmegen ha`lsizliklerin tabi’w
- Qa`wipsizlik ma`selesi boyi’nsha ma`mleketlik talaplarg`a juwap beriwi

Qa`wipsizlik analizi’ni’n` tu`rleri

Sistemani’n’ ha`lsiz jerlerin skanerlew:

- Belgili kemshiliklerge qarati’lg`an
- Avtomatlasti’ri’li’wi’ mu`mkin
- Ekspertlardan minimal mug`darda jumi’s talap yetedi

Test tu`rdegi sistemani’ buzi’w ha`reketleri:

- Belgili ha`m belgili bolmag`an kemshiliklerge qarati’lg`an
- Joqari’ da`rejedegi ekpertlardi’ shaqi’ri’wdi’ talap yetedi
- Ayri’m jag`daylarda ma`mleketlik ni’zamlardi’n` yaki ka`rxanani’n` ishki ta`rtip qag`i’ydalari’ni’n` buzi’li’wi’na ali’p keledi

IT qa`wipsizliginin` auditi’:

- Qa`wipsizlik oblasti’ndag`i’ siyasat ha`m proceduralarg`a qarati’lg`an
- Ishki ta`rtip-qag`i’ydalardi’ iske asi’ri’w ushi’n tiykar boli’p tabi’ladi’

***Tarmaq qa`wipsizligi jag`dayi’n analiz qi’li’wda ha`lsiz jerlerdi skanerlew usi’li’.*** Skanerlew procesin islep shi’g`i’w:

- ha`lsiz jerlerdi tabi’w
- tabi’lg`an ha`lsizliklerge qa`wip da`rejesin beriw
- saplasti’ri’lmag`an kemshiliklerdi tabi’w
- qa`wipsizlik jag`dayi’n jaqsi’law ushi’n waqi’t grafigin ani’qlaw

Tarmaq qa`wipsizligin analiz qi'li'wda test tu`rde sistemag`a kirip ko`riw. Usi' tekseriw maqsetinde sistemani' buzi'w tabi'sli' boli'wi' ushi'n to`mendegiler kerek:

- Tarmaq yaki sistemani' buzi'p kirmekshi bolg`an shaxsti'n` ha`reketlerin boljap ko`riw
- Tarmaq yaki sistema qa`wipsizliginde kemshilikler tabi'n`
- Hu`jim qi'lmaqshi' bolg`an shaxs usi' kemshiliklerden qalay paydalani'wi' mu`mkinligin aldi'nan biliw
- Woqi'w, modifikaciya yetiw yaki joq qi'li'w ruxsat yetilgen resurslardi' tabi'n`
- Hu`jim ani'qlang`an ba?
- Hu`jimnin` signaturasi'n ha`m xarakteristikasi'n berin`
- Usi'ni'slari'n`i'zdi' berin`

Analiz na`tiyjeleri boyi'nsha qa`wipsizliktin` uli'wma sharalari'n islep shi'g`i'w. Informaciyali'q razvedkag`a qarsi' sharalar:

- Internette registraciya qi'li'w ushi'n tek g`ana za`ru`r bolg`an informaciyani' berin`
- Korporativ web saytti' tez-tezden ko`zden keshirip, konfidencial bolg`an informaciyalardi' ani'qlan`
- Web te ja`riyalaw ha`m registraciya qi'li'w ushi'n tek g`ana lawazi'mi'n`i'z tiykari'nda ashi'lg`an yelektron adresin`izdi ko`rsetin`
- Ashi'q forumlardan paydalani'w qag`i'ydalari'n belgileytug`i'n buyri'q shi'g`ari'n`

***Portlardi' skanerlew na`tiyjesinde qanday informaciyani' qolg`a kiritiwimiz mu`mkin?*** A`dette skanerlew na`tiyjesinde to`mendegi informaciyani' ali'wg`a boladi':

- «ashi'q», «ti'n`lanatug`i'n» portlar sistemai

- baylani’sti’ u`zip taslaytug`i’n portlar sistemai

Portlardi’ skanerlewge qarsi’ sharalar:

- Trafikti’ fil`trlawdi’n` ko`p da`rejeli tu`rin wornati’w
- Uzilis yaki kompрometaciya bolg`an jag`dayda is rejesi
- Ruxsatsi’z sistemag`a kiriwlerdi ani’qlaw rejimin wornati’w
- Tek g`ana za`ru`r bolg`an xi’zmetlerdi ashi’p qoyi’w

Uzaqdag`i’ uzel tuwrali’ to`mendegi informaciya ali’ni’wi’ mu`mkin: TCP juwaplari’, ashi’q portlar, bannerler, xi’zmetler, operacion sistema xaqqi’ndag`i’ informaciya

Test (tekseriw) tu`rde sistemag`a ruxsatsi’z kiriw. Test tu`rde sistemag`a kiriw mi’sallari’: ha`lsiz jerlerdi avtomatik tu`rde skanerlew, parollerge hu`jim jasaw, xi’zmet ko`rsetiwden bas tarti’w, qosi’mshalar ha`m mag`li’wmatlar bazasi’na hu`jimler, tarmaqti’ analizlew.

Tarmaq trafigin analiz qi’li’w – hu`jim qi’li’wshi’ni’n` tarmaq tu`yinleri arasi’ndag`i’ baylani’sti’ ti’n`lap turi’w mu`mkinshiligi.

Hu`jim qi’li’wshi’ shaxs to`mendegi ha`reketlerdi wori’nlawi’ mumkin: tu`yindegi informaciyani’ ashi’p taslaw, tarmaq monitori’n wornati’w, tarmaq arqali’ uzati’latug`i’n konfidencial informaciyani’ analiz qi’li’w quri’lmasi’nan paydalani’w, ali’ng`an mag`li’wmatlardan basqa tu`yinlerdi kompрometaciya qi’li’w ushi’n paydalani’w.

Tarmaqti’ analiz qi’li’wg`a qarsi’ sharalar.

Mag`li’wmatlardi’ qorg`aw ushi’n kriptografiyali’q metodlardan paydalani’w, koncentrator worni’na kommutatordan paydalani’w, tiykarg`i’ tarmaq quri’lmlardi’ qorg`aw, tarmaq analizatori’nan paydalani’wdi’ ruxsat etpew, tez-tezden skanerlew

II BAP BOYINSHA JUWMAQ

Yekinshi bapta informaciya qa’wipsizligin ta’miyinlewdin’ apparatli’q-programmali’q qurallari’, informaciyani’ qorg’awdi’n’ tiykarg’i’ apparatli’q qurallari’, mag’li’wmatlardi’ qorg’awdi’n’ ja’rdemshi apparatli’q qurallari’, informaciyalardi’ qorg’awdi’n’ tiykarg’i’ programmali’q qurallari’, autentifikaciyalawdi’ ta’miyinlew jollari haqqi’nda so’z yetiledi.

Jeke kompyuterlerde informaciya qa’wipsizligin ta’miyinlew jollari’, viruslar menen gu’resiw usi’llari’, jeke kompyuterdi viruslardin’ destruktiv ta’sirinen qorg’aw, informaciyali’q sistemalarda informaciya qa’wipsizligi siyasati’n a’melge asi’ri’w, informaciyali’q sistemani’n` qa`wipsizlik jag`dayi’n analizlew, qa`wipsizlik analizi’ni’n` tu`rleri, tarmaq qa`wipsizligi jag`dayi’n analiz qi’li’wda ha`lsiz jerlerdi skanerlew usi’li’ ha’m tag’i’ basqalar haqqinda so’z etiledi.

III. INFORMACIYA QA’WIPSIZLIGIN TA’MIYINLEWDIN’ KRIPTOGRAFIYALI’Q METODLARI’

3.1 Kriptografiya tu’sinigi ha’m woni’n’ rawajlani’w tariyxi’

Informaciyani’ bo’ten adam ruxsatsi’z woqi’y almawi’ ushi’n wo’zgertilgen halda keltiriw adamzatti’ a’yyemgi waqi’tlardan beri qi’zi’qi’rg’an. Kriptografiya tariyxi’ insan tilinin’ tariyxi’ menen bir jasta desek te boladi’. Jazi’wdi’n’ payda boli’wi’ni’n’ wo’zi – bul kriptografiyli’q sistemalardi’n’ payda boli’wi’ degenimiz, ha’m bul sistemalardan tek g’ana sanawli’ adamlar bilgen. A’yemgi Yegipet, a’yemgi Indiyani’n’ bizge jetip kelgen kitaplari’ bug’an mi’sal bola aladi’.

Kriptografiya tariyxi’n sha’rtli tu’rde 4 basqi’shqa bo’liwge boladi’

1) a’piwayi’ kriptografiya

2) formal kriptografiya

3) ilimiy kriptografiya

4) kompyuterli kriptografiya

A’piwayi kriptografiyag’a (XVI a’sir basi’) dushpannan shifrlang’an tekst mazmuni’n jasi’ri’w ushi’n qa’legen (a’dette primitiv) jollardan paydalani’w ta’n. Baslawi’sh basqi’shlarda informaciyani’ qorg’aw ushi’n kodlaw ha’m steganografiyadan paydalani’lg’an, wolar kriptografiyag’a jaqi’n, biraq birdey yemes.

Paydalani’latug’i’n shifrlardi’n’ ko’pshiligi wori’nlari’n almasti’ri’w yaki monoalfavitli worni’na qoyi’w usi’llari’na ali’p kelinedi. Yen’ birinshi tariyxta qalg’an mi’sal boli’p Cezar shifri’ yesaplanadi’. A’yemgi Rimda Yuliy Cezar ta’repinen doslari’na jollag’an xabarlari’n ha’zirgi ku’nde Cezar shifri’ dep atalatug’i’n shifrlaw jollari’ menen a’melge asi’ri’lg’an. Bul shifrda da’slepki teksttin’ ha’r bir ha’ribi wonnan keying bir neshe poziciyada turg’an ha’ripke almasti’ri’w a’melge asi’ri’ladi’.

Polibian dep grek filosofi’ Polibiy ati’ menen atalatug’i’n ja’ne bir shifrda tosi’nanli’ tu’rde tolti’ri’lg’an kvadrat keste ja’rdeminde uli’wma monoalfavitli

almasti’ri’w qollani’lg’an. Grek alfaviti ushi’n bul 5x5 wo’lshemdegi keste. Bunda ha’r bir ha’rip sol kvadratta woni’n’ asti’nda jaylasqan ha’ripke almasti’ri’lg’an. Soni’n’ menen birge steganografiya, Scitala usi’li, yag’ni’y xabarlardi’ shifrlawda scitala dep atalatug’i’n cilindr ja’rdeminde jasi’ri’p jazi’w usi’li’ qollani’lg’an.

Formal kriptografiya basqi’shi’ (XV a’sir aqi’ri’ - XX a’sir basi’) formallasti’ri’lg’an ha’m qoldan deshifrlawg’a sali’sti’rmali’ tu’rde turaqli’ bolg’an shifrlardi’n’ payda boli’wi’ menen baylani’sli’.Yevropa ma’mleketlerinde wolar Ulli’ Tikleniw da’wirinde ilim ha’m sawdani’n’ rawajlani’wi’ informasiyani’ isenimli qorg’aw mu’tajligi payda bolg’anda islep shi’g’i’lg’an. Bunda ju’da’ a’hmiyetli rol’di Leon Batista Al’berti, Italiya arxitektori’ woynag’an. Wol birinshiler qatari’nda ko’palfavitli almasti’ri’wdi’ usi’ng’an. Bul shifr XVI a’sirdin’ diplomati’ Blez Vijiner ati’n alg’an ha’m izbe–iz da’slepki tekst ha’riplerin gilt penen “qosi’w” arqali’ a’melge asi’ri’lg’an. Bul procedurani’ arnawli’ keste ja’rdeminde an’satlasti’ri’w mu’mkin. Woni’n’ “Shifr haqqi’nda traktat” atamadag’’ miyneti (1466 ji’l) kriptologiya boyi’nsha yen’ birinshi ilimiy jumi’s yesaplanadi’. Bul jumi’sta ha’r bir tilde ha’ripler qollani’li’w jiyiligin analiz qi’li’w arqali’ shifrlang’an tekstlerdi qayta tiklew jollari’ ta’riyiplengen ha’m bir neshe shifrlaw usi’li’ usi’ni’lg’an.

Kriptografiya boyi’nsha yen’ birinshi baspadan shi’qqan kitap bolsa “Poligrafiya” dep atali’p, wol 1508 ji’l nemis abbati' Iogannes Trisemus ta’repinen jazi’lg’an. Trisemus shifri’nda shifrlanatug’i’n tekst ha’ripleri aldi’nnan kelisilgen so’zlerge almasti’ri’lg’an. Djovanni Batista Portani’n’ “Si’rli’ xat almasi’w haqqi’nda” kitabi’nda shifrlawdi’n’ bigrammali’q metodi’ usi’ni’lg’an boli’p, wonda ha’r bir tekst ha’riplerinin’ jupli’g’i’ simvolli’q-geometriyali’q figurali’q belgilerge almasti’ri’w joli’ tu’sindirilgen.

XVII a’sirdin’ Angliyali’q filosofi’, ilimpazi’ Frensis Bekon shifrlawg’a qoyi’latug’i’n talaplardi’ islep shi’qqan. 1790 ji’l Tomas Djeffersonni’n’ shifrlawshi’ mashinasi’nda ko’palfavitli’ tekst ha’riplerinin’ wori’nlari’n almasti’ri’w shifri’n a’melge asi’ri’wshi’ mexanizmdi islep shi’qqan. Djefferson mashinasi’ni’n’ ideyasi’ni’n’ jetilistirilgen varianti’n islep shi’g’i’w maqsetinde

1891 ji’l Etyen Bazeri ta’repinen “Bazeri cilindri” dep atalg’an mashina islep shi’g’i’lg’an.

Wonnan ti’sqari’ Fridrix Kazisskiy “Jasi’ri’n jazi’w ha’m deshifrlaw iskusstvosi’ kitabi’nda Vijener shifri’ tu’rindegi shifrlaw joli’ menen wo’zgertilgen xabarlardi’ qayta tiklew jollari’ ta’riyiplengen. Gollandiyali’q Ogyust Kerkgoffsti’n XIX a’sirdin’ 80-ji’llari’nda baspadan shi’g’arg’an ″A’skeriy kriptografiya” kitabi’ bolsa kriptografiyani’n’ rawajlani’wi’na wo’zinin’ salmaqli’ u’lesin qosti’. Kerkgoff kriptografiyani’n’ yen’ tiykarg’i’ ni’zami’n tasti’yi’qlag’an, wol da bolsa shifrdi’n’ si’rli’li’g’i’ woni’n’ algoritmi yemes, ba’lki gilti menen ani’qlani’wi’ kerek.

A’piwayi, soni’n’ menen turaqli’ ko’palfavitli almasti’ri’w shifri’ boli’p Pleyfer shifri’ yesaplanadi’. Bul shifr XIX a’sir basi’nda Charlz Wicton ta’repine islep shi’g’i’lg’an. Soni’n’ menen birge Wicton bul usi’ldi’ yele de jetilistirgen ha’m “yekilik kvadrat” usi’li’n usi’ng’an. Pleyfer ha’m Wicton shifrlari’ birinshi ja’ha’n uri’si’na shekem paydalani’li’p kelgen, sebebi wolardi’ qoldan qayta tiklew ju’da’ qi’yi’n bolg’an.

Al ilimiy kriptografiyadan aldi’ng’i’ kriptografiyani’n’ yen’ axi’rg’i’ jetiskenligi boli’p ja’ne de kripto turaqli’li’qti’ ku’sheytken ha’m de shifrlaw procesin avtomatlasti’ri’w (mexanizaciyalaw) imkaniyati’n bergen rotorli’ kriptosistemalar bolg’an. Bunday sistemalardi’n’ yen’ birinshileri qatari’nda 1790 ji’li’ Tomas Djefferson (keyinshelik AQSh prezidenti) jaratqan mexanikali’q mashina boli’p tabi’ladi’. Bul mashina ja’rdeminde ko’p alfavitli’ almasti’ri’w aylani’p turg’an ha’m de ishine almasti’ri’w a’meli qoyi’lg’an rotorlardi’n’ wo’z ara jaylasi’wi’ni’n’ variaciyasi’ ja’rdeminde a’melge asi’ri’ladi’.

Rotorli’ mashinalarsi’n’ a’meliyatta ken’ tarqali’wi’ tek XX a’sirdin’ basi’nda g’ana baslang’an. Yen’ birinshi a’meliyatta bul maqsette qollani’li’p baslag’an mashina boli’p nemis mashinasi’ Enigma boli’p tabi’ladi’. Bul mashina 1917 ji’l Edvard Hebern ta’repinen islep shi’g’i’lg’an boli’p, Artur Kirx ta’repinen yele de jetilistirilgen. Rotorli’ mashinalar yekinshi ja’ha’n uri’si’ waqti’nda ju’da’ aktiv qollani’lg’an. Enigma dan basqa Sigaba (AQSh), Turex (Ulli’ Britaniya), Red,

Orange ha’m Purple2 (Yaponiya) ken’ paydalani’lg’an. Rotorli’ sistemalar formal kriptografiyani’n’ yen’ jetilisken formasi’ yesaplanadi’, sebebi ju’da a’piwayi’ jol menen ju’da’ turaqli’ shifrlardi’ a’melge asi’rg’an. Rotorli’ sistemalarg’a kriptohu’jimler tek 40-ji’llarda EEMler payda boli’wi’ menen tabi’sqa yerisip baslag’an.

Ilimiy kriptografiyani’n’ (XX a’sirdin’ 30-40 ji’llari’) yen’ ayri’qsha belgisi – bul kriptoturaqli’li’g’i’ qatan’ matematikali’q tiykarlang’an kriptosistemalardi’n’ payda boli’wi’. 30-ji’llardi’n’ baslari’nda kriptologiyani’n’ ilimiy tiykari’ bolg’an matematikani’n’ bo’limleri ani’q qa’liplesip boldi’. Bul itimalli’qlar teoriyasi’ ha’m matematikali’q statistika, uli’wma algebra, sanlar teoriyasi’. Soni’n’ menen birge algoritmler teoriyasi’, informaciya teoriyasi’, kibernetika rawajlani’p basladi’. Tariyxiy hadiyse boli’p 1949 ji’lda baspadan shi’qqan Klod Shennonni’n’ “Si’rli’ sistemalarda baylani’s teoriyasi’” atamasi’ndag’i’ kitabi’ tabi’ladi’. Bul miynette avtor informaciyani’ kriptografiyali’q qorg’awdi’n’ teoriyali’q principlerin tasti’yi’qlag’an. Shennon “jayi’li’w” ha’m “aralasi’p ketiw” tu’siniklerin kiritken ha’m qa’legen sanda turaqli’ kriptosistemalar jarati’w imkaniyati’n tiykarlap bergen.

60-ji’llarda yen’ tani’qli’ kriptografiyali’q mektepler blokli’ shifrlar jarati’wg’a jaqi’nlag’an, bunday shifrlar rotorli’ kriptosistemalardan da turaqli’, lekin tek g’ana cifrli’ elektron quri’lmalar ja’rdeminde a’melge asi’ri’li’wi’ mu’mkin bolg’an.

XX a’sirdin’ 70-ji’llari’nan baslap kompyuterli kriptografiya payda bolg’anli’g’i’ ku’shli yesaplaw qurallari’ islep shi’g’i’lg’anlig’i’ menen belgilenedi. Bul yesaplaw qurallari’ni’n’ wo’nimdarli’g’i’ u’lken shifrlaw tezliginde bir neshe ta’rtip joqari’ kriptoturaqli’li’qti’ ta’miyinlew ushi’n jeterli bolg’an.

Ku’shli yesaplaw texnikasi’ ja’rdeminde blokli’ shifrlaw a’melge asi’ri’w mu’mkin. 70-ji’llarda DES amerikali’q shifrlaw standarti’ islep shi’g’i’li’p, 1978 ji’lda qabi’llang’an. Bul standartti’n’ avtorlari’ni’n’ biri Xorst Feystel (IBM firmasi’ni’n’ xi’zmetkeri) blokli’ shifrlar modelin ta’riyiplegen, woni’n’

tiykari’nda basqa da wonnan da turaqli’ simmetriyali’q kriptosistemalar payda bolg’an, wolardi’n’ qatari’nda GOST 28147-89 shifrlaw standarti’ DES payda boli’wi’ menen kriptoanaliz usi’llari’ bayi’ti’ldi’, amerikali’q shifrlaw algoritmin hu’jimge ali’w ushi’n bir neshe jan’a kriptoanaliz jollari’ islep shi’gi’lg’an (si’zi’qli’, differencialli’q, h.t.b.) ha’m wolardi’n’ a’melge asi’ri’li’wi’ tek g’ana ku’shli yesaplaw sistemalari’ payda boli’wi’ menen mu’mkin bolg’an.

70-ji’llardi’n’ wortasi’nda zamanago’y kriptografiyada haqi’yqi’y revolyuciya bolg’an, wol da bolsa asimmetriyali’q, yag’niy simmetriyali’q bolmag’an kriptosistemalar payda bolg’an. Bunday kriptosistemalar ta’repler arasi’nda si’rli’ gilt almasi’wdi’ talap yetpegen. Bul tarawda yen’ da’slepki tu’rtki boli’p Witfill Diffi ha’m Martin Xellman ta’repinen 1976 ji’lda baspadan shi’g’ari’lg’an “Zamanago’y kriptografiyani’n’ jan’a bag’darlari’” miyneti bolg’an. Bul kitapta yen’ birinshi ma’rte shifrlang’an informaciyani’ si’rli’ gilciz almasi’wdi’n’ principleri taiyiplengen. Bul avtorlardan biyg’arez asimmetriyali’q kriptosistemalar ideyasi’na Ralf Merkli de kelgen. Bir neshe ji’ldan keyin bolsa Ron Rivest, Ali Shamir ha’m Leonard Adleman RSA dep atalg’an sistemani’ islep shi’qti’. Bul sistema yen’ birinshi a’meliy asimmetriyali’q kriptosistema boli’p tabi’ladi’ ha’m woni’n’ turaqli’li’g’i’ u’lken sanlardi’ fakrorizaciya qi’li’w problemasi’na tayanadi’. Asimmetriyali’q kriptografiya birdenine bir neshe jan’a a’meliy bag’dar ashi’li’wi’na sebepshi boldi’, atap aytqanda elektron cifrli’ imza ha’m elektron aqsha.

80-90-ji’llarda itimalli’q shifrlaw, kvantli’ kriptografiya h.t.b. siyaqli’ absolyut jan’a kriptografiya tarawlari’ payda boldi’. Wolardi’n’ a’meliy qa’dirin an’law yele aldi’mi’zda. Simmetiyali’q kriptosistemalardi’ yele de jetilistiriw de aldi’mi’zdag’i’ wazi’ypa boli’p tabi’ladi’. 80-90-ji’llarda feysteldiki bolmag’an shifrlar (SAFER, RC6 h.t.b.) jarati’lg’an, al 2000 ji’l ashi’q xali’qarali’q konkurs ja’riyalang’annan keyin AQSh-tin’ jan’a milliy shifrlaw standarti’ AES qabi’llang’an.

Ha’zirgi ku’nde jeke kompyuterlerde ha’m de u’lken informaciyali’q sistemalarda informaciyani’ qorg’awdi’n’ kompleksli sharalari’ qollani’ladi’.

Informaciyani’ qorg`aw usi’llari’ olardan duri’s paydalang`an jag`dayda qorg`ali’p ati’rg`an informaciyag`a ji’nayachi’ ta`repinen hu’jim jasaw mu`mkin yemesligine kepillik beriwshi mexanizmler ha`m metodlardi’n` toplami’na tayanadi’.

Bizge belgili, kriptografiyali’q qurallar ha’zirgi waqi’tqa deyin tiykari’nan ma’mleketlik si’rlardi’ qorg’awg’a qarati’lg’an yedi, sol sebepli bul qurallar arnawli’ organlar ta’repinen jarati’lg’an. Bunda joqari’ kriptoturaqli’li’qqa iye bolg’an kriptosistemalar qollani’lg’an, bul bolsa u’lken qa’rejetlerdi talap qi’lg’an.

Keyingi ji’llarda mag’li’wmatlardi’ kriptografiyali’q wo‘zgertiriwdin’ jan’a usi’llari’ intensiv islep shi’g’i’lmaqta, wolar da’stu’riy qollani’wg’a qarag’anda ken’irek tarawlarda paydalani’li’p kelmekte’.

Avtomatlasti’ri’lg’an sistemalarda mag’li’wmatlardi’ qorg’awdi’n’ kriptografiyali’q usi’llari’ yesaplaw texnikasi’ qurallari’nda qayta islenilip yaki ha’r tu’rdegi saqlaw quri’lmalari’nda saqlani’p ati’rg’an mag’li’wmattlardi’ qorg’awda, soni’n’ menen birge baylani’s liniyalari’ arqali’ sistema elementlarine uzati’li’p ati’rg’an mag’li’wmatlardi’ qorg’awda qollani’ladi’. Ha’zirgi waqi’tta ko‘plep ha’r tu’rli shifrlaw usi’llari’ islep shig’i’lg’an ha’m wolardi’ qollawdi’n’ teoriyali’q ha’m a’meliy tiykarlari’ jarati’lg’an.

Informaciyali’q sistemalarda kriptografiyali’q usi’llar ken’ qollani’lmaqta, sebebi kompyuter tarmaqlari’, atap aytqanda Internet tez pa’t penen rawajlanbaqta. Tarmaq arqali’ ma’mleketlik, a’skeriy, biznes ha’m shaxsiy qa’siyetke iye u’lken ko’lemdegi mag’li’wmatlar uzati’lmaqta. Bul mag’li’wmatlarg’a bo’ten shaxslardi’n’ kiriwi mu’mkin yemes. Soni’n’ menen birge, joqari’ quwwatli’ kompyuterlerdin’, tarmaq ha’m neyron yesaplaw texnologiyalari’ni’n’ payda boli’wi’ aldi’n ju’da’ bekkem, a’meliyatta sheshimi joq dep yesaplang’an kriptografiyali’q sistemalardi’n’ abi’royi’n to’menletti. Bil bolsa zamanago’y kriptografiyali’q usi’llardan paydalani’w ju’da’ aktual ekenligin an’latadi.

3.2 Kriptografiyali’q metodlar ha’m wolardan paydalani’w metodikasi’

Zamanago’y kriptografiya informaciya qa’wipsizliginin’ *konfidencialli’q, pu’tinlik, autentifikaciya ha’m ta’replerdin’ avtorli’qti’ inkar yete almasli’qlari’* mashqalalari’n ha’l yetiwshi bilim tarawi’ yesaplanadi’.

Konfidencialli’qti ta’miyinlew degende informaciya menen tani’si’w huquqi’ bolmag’an shaxslardan bul informaciyani’ qorg’aw tu’siniledi.

Qarsi’las ta’repten baqlawda bolg’an baylani’s kanali’ arqali’ uzati’li’p atri’rg’an xabardi’n’ konfidencialli’g’iin ta’miyinlew mashqalasi’ kriptografiyani’n’ da’stu’riy ma’selelerinen yesaplanadi’. A’piwayi’ jag’dayda bul mashqala u’sh subyekt (ta’repler)din’ wo‘zara muna’sibeti si’pati’nda bayan yetiledi. Informaciya iyesi (jo‘netiwshi), qarsi’las ta’repten qorg’aw qi’li’w maqsetinde, ashi’q kanal arqali’ qabi’llawshi’g’a jiberilip atri’rg’an ashi’q mag’li’wmatti’ wo‘zgertedi, yag’ni’y shifrlaydi’.

Uzati’li’p ati’rg’an xabar mag’anasi’ menen tani’si’w huquqi’ joq subyekt qarsi’las ta’repti an’latadi’. Deshifrlaw menen shug‘i’llanatug’i’n kriptoanalitik ha’m qarsi’las ta’rep si’pati’nda qarali’wi’ mu’mkin. Ali’ng’an xabardi’ haqiqiy qabi’llawshi’ *deshifrlaydi*. Qarsi’las ta’rep bolsa qorg’ali’p ati’rg’an xabarg’a iyelik qi’lmaqshi’ boladi’, woni’n ha’reketi *hu’jim ye*saplanadi’. Hu’jim aktiv yaki passiv boli’wi’ mu’mkin.

Passiv hu’jim jasi’ri’n yesitiw, trafikti’ analiz qi’li’w, shifrlang’an xabardi’ qolg’a kiritiw, *deshifrovka qi’li’w*, yag’niy qorg’awdi’ «si’ndi’ri’w»g’a qarati’lg’an ha’reketler yesaplanadi’. Aktiv hu’jimde qarsi’las ta’rep xabardi’ uzati’w procesin toqtati’p qoyi’wi’, wo’tirik xabarlar jo’netiwi yaki shifrlap uzati’li’p ati’rg’an xabardi’ modifikaciya qi’li’wi mu’mkin. Bul aktiv ha’reketler sa’ykes ra’wishte imitaciya qi’li’wg’a ha’m almasti’ri’p qoyi’wg’a uri’ni’w yesaplanadi’.

Gilt shifrlawdi’n’ tiykarg’i’ elementi boli’p, berilgen xabardi’ shifrlawdag’i’ almasti’ri’wlar wol arqali’ a’melge asi’ri’ladi’. A’dette, gilt ha’rip ha’m sanlardi’n’ belgili bir izbe-izliginen ibarat boladi’.

Ha’r bir almasti’ri’w glt menen bir ma’nisli ani’qlanadi’ ha’m belgili bir kriptografiyali’q algoritm arqali’ a’melge asi’ri’ladi’. Shifrlawda bir kriptografiyali’q algoritm h’ar tu’rli rejimlerde qollani’li’wi’ mu’mkin. Sol ta’rtipte ha’r tu’rli shifrlaw usi’llari’ (a’piwayi’ almasti’ri’w, gammalaw ha’m basqalar) a’melge asi’riladi’. Ha’r bir rejimnin’ abzalli’q ha’m kemcshilik ta’repleri bar. Sol sebepli rejimdi tan’law konkret jag’dayg’a baylani’sli’. Deshifrlawdag’i’ kriptografiyali’q algoritm, uli’wma halda, shifrlawdag’i’ algoritmdan pari’q qi’li’wi’ mu’mkin. Bul jag’dayda shifrlawdag’i’ ha’m deshifrovka qi’li’wdag’i’ giltler ha’m sa’ykes tu’spewi mu’mkin. Shifrlawshi’ ha’m deshifrovka qi’li’wshi’ algoritmler jupli’g’i’n kriptosistema, bul algoritmlerdi a’melge asi’ri’wshi’ quri’lmani’ shifrlawshi’ texnika dep ataladi’.

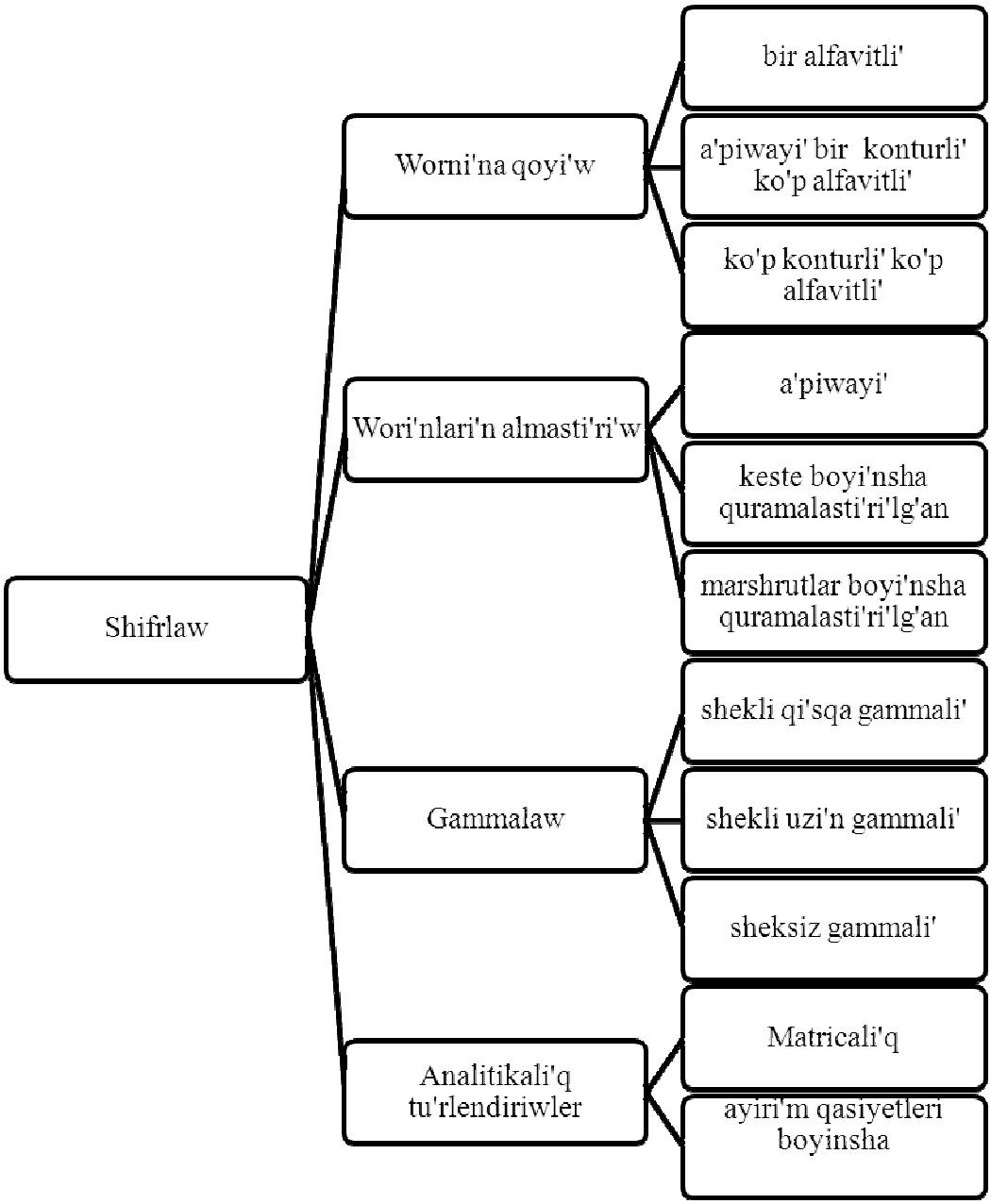
Barli’q jag’daylarda sa’ykes jalg’i’z shifr joq. Shifrlaw usi’li’n, yag’ni’y kriptografiyali’q algoritm ha’m wonnan paydalani’w rejimin tan’law uzati’li’p atri’rg’an informaciyani’n’ qa’siyetlerine (ma’nisi, ko’lemi, su’wretlew usi’li’na, za’ru’riy uzati’w tezligine ha’m basqalar) ha’m de informaciya iyesinin’ informaciyani’ qorg’aw imkaniyati’na (qo‘llani’li’p ati’rg’an texnikali’q qurallari’ni’n’ bahasi’na, qollawdi’n’ qolayli’li’g’Ii’na, islewdin’ isenimliligine ha’m basqalar) baylani’sli’ boladi’.

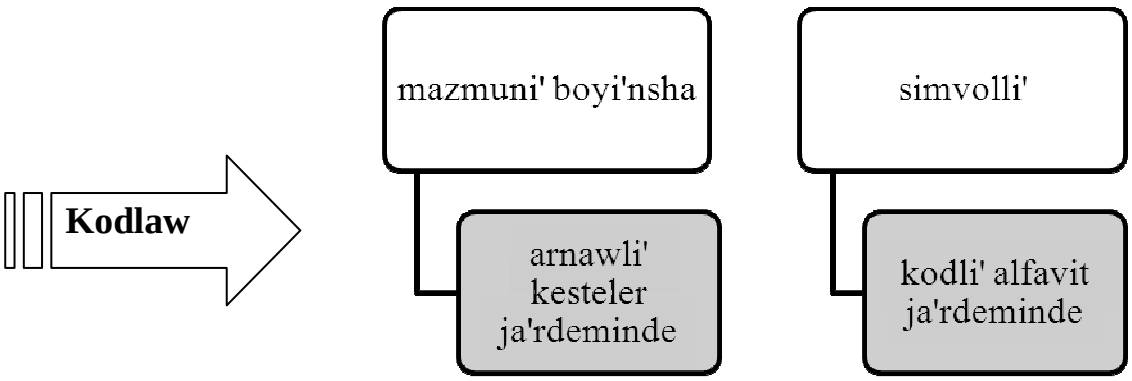
Qorg’alatug’i’n informaciya ha’r tu’rli formalarg’a (tekstli, dawi’sli’, su’wretli ha’m basqalar) iye boli’wi’ mu’mkin. Ha’r bir formani’n’ wo‘zine ta’n qa’siyetleri bar boli’p, shifrlaw usi’li’n tan’lawda woni’ yesapqa ali’w kerek. Shifrlang’an informaciyani’n’ ko’lemi, woni’ talap yetilgen tezlikdte uzati’w ha’m de baylani’s kanali’ni’n’ ha’r tu’rli jag’daylarda beriwshi shawqi’mlardan qorg’alg’anli’g’i’ u’lken a’hmiyetke iye. Bulardi’n’ ba’rshesi kriptografiyali’q algoritmdi tan’lawda ha’m qorg’alg’an baylani’sti’ sho’lkemlestiriwde a’hmiyetli rol’ woynaydi’.

Kriptografiyali’q iskerliktin’ xarakteristikasi’. Ko‘pshilik kriptografiyali’q qorg’aw usi’llari’n qollawda belgili bir informaciya almasi’w za’ru’riyati’ payda boladi’. Ma’selen, informaciya-telekommunikaciya sistemasi’ obyektlerin autentifikaciya qi’li’w identifikaciyalawshi’ ha’m autentifikaciyalawshi’

informaciyalar almasi’wi’ arqali’ a’melge asadi’. Uli’wma jag’dayda, bunday sistemalar obyektleri (subyektlari)nin’ wo‘z ara muna’sibeti belgili bir kelisiwler (*protokollar*)g’a a’mel qi’li’ng’an halda boladi’. Obyekt (subyekt)lardi’n’ belgili bir maqsetke yerisiwi ushi’n izbe iz wori’nlanatug’i’n a’melin formal tu’rde protokol dep ataw mu’mkin. Qo‘yi’lg’an maqset protokoldi’n’ du’zilisin ha’m qollaw qa’siyetlerin belgileydi.

Informaciyani’ jasi’ri’wdi’n` tiykarg`i’ kriptografiyali’q metodlari’ni’n` klassifikaciyasi’





Basqa kriptografiyali'q metodlar

- Steganografiya
- Basqa tu`rleri:
    1. Kesiw-jayi'w
        a. Ma`nisi boyi'nsha
        b. Mexanikali'q
    2. Qi'si'w-ken`eytiw

Kriptograf ha`m kriptoanalitiktin` wazi'ypalari'

Meyli, informaciya almasi'w procesinin` yeki qatnasi'wshi'si' (uzati'wshi' A ha`m qabi'llawshi' V) jasi'ri'n baylani's jasawg`a ha`reket yeCin.

*Xabardi' uzati'wshi'ni'n` wazi'ypasi':* xabar ***T*** jarati'w ha`m woni' qabi'llawshi'g`a uzati'w.

*Xabardi' qabi'llawshi'ni'n` wazi'ypasi'*: uzati'lg`an xabardi' ali'w ha`m woni'n` mazmuni'n tu`siniw.

Uzati'wshi' A xabardi' ***E*** *algoritmi* ja`rdeminde sonday qi'li'p wo`zgertiwi kerek, woni' qabi'llawshi'dan basqa hesh kim qayta tikley almasi'n. Bunday wo`zgertiw xabar ***T***-ni' *shifrlaw*, al bul procedurani'n` na`tiyjesi *shifrotekst* ***T'*** dep ataladi'. Da`slepki (tiykarg`i') tekst ***T***, shifrotekst ***T'*** ha`mde shifrlaw algoritmi ***E*** arasi'ndag`i' baylani's to`mendegi formula menen beriledi:

$$T' = E(T).$$

Shifrlang`an xabar T' baylani’s kanali’ arqali’ uzati’ladi’.

Xabardi’n` mazmuni’n biliw ushi’n qabi’llawshi’ aldi’n woni’ qayta tiklewi kerek, yag`ni’y shifrotekst T' –qa deshifrlaw algoritmi D qollani’ladi’. Demek, mag`li’wmatlardi’ deshifrlaw

$$T = D(T')$$

ten`lemesi menen beriledi.

Kriptoanalitiktin` wazi’ypasi’:

- T' *x*abari’n deshifrlaw, yag`ni’y tekstti toli’g`i’ menen yaki woni’n` bo`legin ashi’w yaki keminde qolg`a kiritilgen xabardi’n` ishinen tabi’lg`an ayri’m ni’zamli’li’qlarg`a tiykarlani’p, tekst mazmuni’ haqqi’nda mag`li’wmatqa iye boli’w;
- Jan`adan sonday xabar $\tilde{T}'$ jarati’w, woni’ xaqi’yqi’y adresat (qabi’llawshi’) xaqi’yqi’y dep qabi’llasi’n;

  Shifrdi’ ashi’w dep, joqari’da ko`rsetilgen qa`wiplerdin` hesh bolmasa birewin tabi’sli’ a`melge asi’ri’w tu`siniledei. Birinshi qa`wip a`melge asi’ri’lg`anda xabardi’n` si’rli’li’g`i’n, al yekinshisi xabardi’n` pu`tinligin (haqi’yqi’yli’g`i’n) buzg`an boladi’.

***Kriptografti’n` wazi’ypasi’*** mag`li’wmatlardi’ uzati’wdi’n` si’rli’ (jasi’ri’n) ha`m autentikli’q sistemasi’n islep shi’g`i’w boli’p tabi’ladi’.

Autentiklik (autentichnost`) – bul kriptosistemanin` wo`tirik mag`li’wmatlardan qorg`alg`anli’g`i’.

Si’rli’li’q (sekretnost`) - bul jasi’ri’n mag`li’wmatlardi’n` mazmuni’ menen sankciyasi’z(ruxsatsi’z) tani’si’wdan kriptosistemanin` qorg`alg`anli’g`i’

Kriptoalgoritmler – bul «si'r» ja`rdeminde berilgenlerdi wo`zgertiw algoritmleri. Kriptoalgoritmnin` sapa jag`i'nan tiykarg`i' parametri boli'p qarsi' ta`reptin` bul «si'rdi'» ashi'wg`a qarati'lg`an ha`reketlerine shi'damli'li'g`i', basqasha aytqanda woni'n` turaqli'gi' yesaplanadi'. Kriptoanalizge bolg`an bunday shi'damli'q turaqli'li'q dep ataladi'.

Simmetriyali'q ha`m asimmetriyali'q kriptosistemalar

Ha`zirgi kunde **kriptosistemani'** yeki klassqa aji'rati'w mumkin:

• simmetriyali'q bir giltli (si'rli' giltli);

• asimmetriyali'q yeki giltli (ashi'q giltli).

Simmetriyali'q sistemalarda to`mendegi eki mashqala payda boladi':

1) Informaciya almasi'wda qatnasi'wshi'lar kanday jol menen si'rli' giltti bir-birewine uzati'wi' mumkin?

2) Jiberilgen xabardi'n` haqi'yqi'yli'g`i'n qanday ani'qlasa boladi'?

Bul mashqalalardi'n` sheshimi ashi'q giltli sistemalarda tabi'ladi'.

Ashi'q giltli asimmetriyali'q sistemade yeki gilt kollani'ladi'. Birinen yekinshisin esaplaw usi'llari menen ani'qlap bolmaydi'.

Birinshi gilt informaciya jiberiwshi ta`repinen shifrlawda isletilse, yekinshisi informaciyani' qabi'llawshi' ta`repinen informaciyani' tiklewde qollani'ladi' ha`m wol si'r saqlani'wi' sha`rt.

Kriptosistemanin` turaqli'li'gi' woni'n` gilti menen ani'qlanadi' ha`m bul kriptoanalizdin` tiykarg`i' qag`i'ydalari'nan biri boli'p yesaplanadi'.

Simmetriyali'q kriptosistemaler

Kriptografiyali'q algoritm, basqasha aytqanda shifr, matematikali'q funkciya boli'p, informaciyani' shifrlawda ha`m deshifrlawda qollani'ladi'**.**

Gilt — bul kriptografiyali'q tu`rlendiriwler algoritminin` bazi'-bir parametrlerinin` si'rli' ko`rinisi boli'p, barli'q algoritmlerden jalgi'z varianti'n

tanlaydi’. Giltlerge qaray isletiletugi’n tiykarg`i’ ko`rsetkish boli’p kriptoturaqli’li’q yesaplanadi’.

Simmetriyali’q kriptoalgoritmlerge to`mendegiler kiredi:

• worni’na qoyi’w;

• wori’nlari’n almasti’ri’w;

• gammalaw;

• analitikali’q tu`rlendiriwler.

Worni’na qoyi’w shifrlaw usi’li’ boyi’nsha tekst belgileri paydalani’li’p ati’rg`an yaki baska bir alippe belgilerine almasti’ri’lali’.

Wori’nlardi’ almasti’ri’w shifrlaw usi’li’ boyi’nsha tekst belgilerinin` teksttin` belgili bir bo`legi shen`berinde arnawli’ kag`i’ydalar ja`rdeminde wori’nlari’ almasti’ri’ladi’.

Gammalaw usi’li’ boyi’nsha tekst belgileri shifrlaw gammasi’ belgileri, yag`ni’y tosi’nanli’ belgiler izbe-izligi menen birlestiriledi.

**Analitikali’q tu`rlendiriwler** usi’li’ boyi’nsha tekst belgileri analitikali’q formulalar ja`rdeminde wo`zgertiriledi, maselen, vektordi’ matricaga ko`beytiw ja`rdeminde. Bul jerde vektor teksttegi belgiler izbe-izligi, matrica bolsa gilt si’pati’nda xi’zmet yetedi.

Shifrlawdi’n` worni’na qoyi’w (zamena, podstanovka) metodi’

Shifrlawdi’n` yen` an`sat joli’. Bunda shifrlani’wshi’ tekst simvollari’ usi’ (bir) alfavitten yaki bir neshe alfavitten ali’ng`an basqa simvollarg`a almasti’ri’ladi’.

Bir alfavitli almasti’ri’w. Bunda shifrlani’wshi’ tekst simvollari’ni’n` worni’na tuwri’dan-tuwri’ usi’ yaki basqa bir alfavit simvollari’ qoyi’ladi’ (almasti’ri’ladi’).

Bul tu`rdegi usi’llarg`a Cezar usi’li’, Affin sistemaindegi Cezar usi’li’ ha`mde tayani’sh so`zli Cezar usi’li’ ha`m basqalar kiredi.

Cezar usi'li'n da almasti'ri'wshi' ha`ripler k ha`m ji'lji'w menen ani'qlanadi'. Yuliy Cezar k= 3 bolg`anda usi' usi'ldan paylalangan.

Bul usi'ldi'n` matematikali'q ani'qlamasi' to`mendegishe:

Cezar sistemasi' dep ashi'q tekstti'n` (x0, *xi* ,..,xn-i) n-grammasi'n to`mendegi qag`i'yda boyi'nsha

$$y_i=C_k(x_i),\ 0\le i<n.$$

shifrlang`an tekst (u0 ,yi ,...,yn.i) n-grammasi'na aylandi'ratug`i'n mono (bir) alfavitli worni'na qoyi'w metodi'na ayti'ladi'.

Wori'nlari'n almasti'ri'w (perestanovka) usi'llari'

Ani'qlama. (0, 1, 2, …,N-1) pu`tin sanlar ko`pliginde sanlardi'n` σ-wori'nlari'n almasti'ri'w dep woni' qayta ta`rtiplestiriwge ayti'ladi', bunda pu`tin *i*-sani' *i*—shi poziciyadan σ(*i)* –poziciyag`a to`mendegi qag`i'yda boyi'nsha ko`shiriledi:

$$\sigma = (\sigma(0), \sigma(1),... \sigma(N-1))$$

Wori'nlardi' almasti'ri'w usi'li' yen` a`piwayi' ha`m yen` a`yemgi usi'llar qatari'na jatadi'. Bunda ashi'k teksttegi ha`ripler baska ha`riplerge almasti'ri'lmaydi', ba`lki wlardi'n` wri'nlari' almasti'ri'ladi'.

Mi'sali', a`piwayi' bag`analar boyi'nsha wori'n almasti'ri'wda da`slepki ashi'q tekst qatarlar boyi'nsha arnawli' bag`analarg`a jazi'p shi'g`i'ladi'. Shifr-tekst ha`riplerdi bag`analar boylap woqi'w arqali' payda boladi'. Qayta ashi'w ha`m sol ta`rtipte wori'nlanadi'. Shifr-tekst bag`analar boyi'nsha jazi'p shi'g`i'ladi'. Ashi'q tekst gorizontal boyi'nsha woqi'w arkali' payda boladi'.

Wori'nlardi' almasti'ri'w usi'llari'na to`mendegi usi'llar kiredi:

— shifrlawshi' keste;

— magiyali'q (si'yqi'rli') kvadrat

Vijener kestesi. XVI a'sirde fransuz diplomati' Vijiner ta'repinen jarati'lg'an shifrlaw sistemasi' 1586-ji'lda baspadan shi'qqan. Wol tani'qli' ko'p alfavitli'

sistema yesaplanadi’. Vijiner sistemasi’ Cezar shifrlaw sistemasi’na qarag’anda bekkemlew yesaplani’p, wonda gilt ha’ripten ha’ripke almasti’ri’ladi’. Bunday ko‘p alfavitli almasti’ri’w shifri’n shifrlaw kestesi arqali’ ani’qlaw mu’mkin. To’mendegi kestelerde rus ha’m lati’n alfavitleri ushi’n sa’ykes keliwshi kesteler ko‘rsetilgen. Bul kestelerden tekstti shifrlaw ha’m woni’ ashi’w ushi’n paydalani’ladi’. Kestenin’ yeki kiriwi boli’p:

– joqari’ qatardag’i’ ha’riplerden kiriwshi ashi’q jazi’w ushi’n paydalani’ladi’.

– shep bag’anada bolsa gilt so‘zi jaylasadi’.

Ashi’q tekstti shifrlawda bul tekst bir qatarg’a jazi’ladi’. Woni’n’ asti’ndag’i’ qatarin’da gilt so‘z jaylasti’ri’ladi’. Yeger gilt so‘zdin’ uzi’nli’g’i’ qi’sqa bolsa, bu’ so‘z ashi’q teksttin’ aqi’rg’I’ ha’ripineshe ta’kirarlap jazi’ladi’. Shifrlaw procesinde kestenin’ joqari’ bo’leginde jaylasqan ashi’q teksttin’ ha’ripi tabi’ladi’ ha’m shep bo’lekten gilt so‘zdin’ ha’ribi tan’lanadi’. Qatar ha’m bag’ana kesilisken ketektegi ha’rip berilgen ha’ripti almasti’radi’

Xabar	M	A	G	I	S	T	R
Gilt	B	O	L	B	O	L	B
Shifrtekst	N	O	R	J	G	E	S

Gammalaw metodi'

Bul metod basqasha additiv metod dep ataladi' ha`m bunda xabarlardi' shifrlawda shifrlanatug`i'n tekst simvollari' gamma dep atalatug`i'n arnawli' bir izbe-izliktin` simvollari' menen izbe-iz qosi'li'p bari'ladi'.

Gammalaw bir neshe jol menen a`melge asi'ri'ladi', mi'sali' to`mendegi formula ja`rdeminde

$$c_h = t_o \text{ XOR } t_g,$$

bunda c_h, t_o, t_g - tiyisli tu`rde shifrlang`an simvoldi'n`, da`slepki simvoldi'n` ha`m gammani'n` ASCII kodlari', XOR –("isklyuchayushee ili")

Tekstti deshifrlaw da sol formula ja`rdeminde ori'nlanadi':

$$t_o = c_h \text{ XOR } t_g,$$

Gammani' psevdo-tosi'nanli' sanlar (PC) datchigi ja`rdeminde jarati'wg`a boladi'.

Bul metodta gilt boli'p gamma xi'zmet qi'ladi'. Gammalaw metodi'ni'n` turaqli'gi' gamma periodi'ni'n` uzi'nli'g`i' menen ani'qlanadi'. Zamanago`y PC-larda jarati'latug`i'n sheksiz gammalar (teoriyada) shifrlang`an teksttin` sheksiz turaqli'gi'n ta`miyinlew mu`mkinshiligin beredi.

Analitikali'q tu`rlendiriwler metodi'

Informaciyani' jetkilikli da`rejede jasi'ri'wdi' shifrlawdi'n` analitikali'q tu`rlendiriwlerden paydalani'w usi'li' ta`miynlewi mu`mkin. Mi'sali', matricalar algebrasi', atap aytqanda matricani' vektorg`a ko`beytiw metodi'.

Bunda gilt si’pati’nda n*n wo`lshemli kvadrat matrica ||a|| xi’zmet qi’ladi’. Tiykarg`i’ tekst uzi’nli’g`i’ n simvoldan bolg`an bloklarg`a bo`linedi. Ha`r bir blok n-wo`lshemli vektor dep qaraladi’. Blokti’ shifrlaw processi bolsa ||a|| matricani’ da`slepki vektorg`a ko`beytiw na`tiyjesinde jan`a n-wo`lshemli vektor (shifrlang`an blok) tabi’wdan ibarat boladi’.

Tekstti deshifrlaw processi da`l sonday wo`zgertiwlerdi a`melge asi’ri’w na`tiyjesinde a`melge asi’ri’ladi’, biraq bunda ||a|| matricani’n` kerisi menen isleymiz (bunda matrica determinanti’ D= 0 bolmawi’ kerek).

Informaciyani’ qorg`awdi’n` jeterlilik principi

Informaciyani’ jeterli da`rejede qorg`alg`an dep ayti’w mumkin, yegerde woni’ ashi’w ushi’n ketetug`i’n qa`rejetler informaciyani’n` bahasi’nan joqari’ bolsa.

Dag`aza qi’li’ng`an ashi’k gilt tiykari’nda jabi’q gilt jarati’wg`a ketetug`i’n wortasha waqi’t kodlasti’ri’w algoritminin` kriptoturaqli’li’gi’ dep ataladi’.

XIX a`sirde gollandiyali’q ilimpaz **Kerkxoff** kriptografiyali’q sistemalarg`a qoyi’latug`i’n tiykarg`i’ talap si’pati’nda ***shifrdi’n` si’rli’li’g`i’ woni’n` algoritminin` si’rli’li’g`i’nda yemes, ba`lki woni’n` giltinin` si’rli’li’g`i’nda*** degen.

Bir neshe usi’ldi’ biriktirip shifrlaw usi’llari’ (kombinirovanni’e metodi’)

Shifrdi’n` shi’damli’li’g`i’n ta`miynlewde bir neshe usi’ldi’ izbe-iz qollani’w effektiv boli’p tabi’ladi’. Bunday shifrlawdi’n` shi’damli’li’g`i’ S qollani’li’p ati’rg`an ha`r bir usi’ldi’n` shi’damli’li’qlari’ni’n` ko`beymesinen to`men bolmaydi’.

$$S >= S_1*S_2*...*S_k$$

Yegerde qanday da bir usi’ldi’ qollang`anda shifrlaw shi’damli’li’g`i’ S ten to`men bolmasa, wonda bul usi’ldi’ basqa usi’l menen kombinaciya qi’li’w za`ru`rligi

$$R > R_1+R_2+ ... +R_k$$

(R_i - i-shi usi'lg`a ketetug`i'n miynet ko`lemi, R - S ten to`men bolmag`an turaqli'li'qti' ta`miynlewshi usi'ldi'n` miynet ko`lemi)

jag`dayda g`ana wo`zin aqlaydi'.

Asimmetriyali'q (ashi'q giltli) kriptosistemaler

Simmetriyali'q kriptosistemalarda mag`li'wmatlardi' jasi'ri'w ushi'n shifrlawda jasi'ri'n giltten paydalani'ladi'. Shifrlang`an tekstti ashi'wda da sol bir giltten paydalani'ladi'. Bul giltti tek g`ana aldi'nnan kelisip alg`an xabardi' jiberiwshi ha`m qabi'llawshi' biledi. Bunday kriptosistemaler basqasha jabi'q giltli dep ataladi'. Si'rli' giltti qolg`a kiritken basqa adamlar ha`m xabardi'n` da`slepki tekstin an`sat qayta tikley aladi'.

Ashi'q gilt ***K*** ja`rdeminde shifrlaw (asimmetriyali'q kriptoalgoritm) to`mendegishe beriledi:

$$E_K(M)=C$$

Ashi'q ha`m jabi'q gilt birdey bolmasa da, jabi'q gilt ja`rdeminde deshifrlaw to`mendegishe berilenedi

$$D_K(C)=M$$

Geypara waqi'tlari' xabarlar jabi'q gilt penen shifrlanadi', al wolardi' ashi'wda bolsa yekinshi gilt qollani'ladi'.

Simmetriyali'q usi'llardi'n` kemshiligi xabar almasi'wdan aldi'n adresatlar gilt xaqqi'nda bir-birewine xabar beriwi ushi'n isenimli baylani's kanali'n tabi'wi' kerek boladi'. Sol sebepli, mi'sali' Internet arqali' to`lemler ushi'n, basqa kriptoalgoritmler qollani'ladi'.

Kriptografiyali’q qorg`awdi’n` effektivligin ashi’q giltli, basqasha aytqanda asimmetriyali’q (simmetriyali’q bolmag`an) kriptosistemaler ta`miynleydi. Bunday sistemalarda mag`li’wmatlardi’ shifrlawda bir giltten, al deshifrlawda – basqa bir giltten paydalani’ladi’.

Birinshi gilt ashi’q boli’p, ja`riyalanadi’. Bul giltten qalegen sistema paydalani’wshi’lari’ mag`li’wmatlari’n shifrlawda paydalani’wi’ mu`mkin. Biraq shifrlang`an mag`li’wmatlardi’ usi’ gilt ja`rdeminde ashi’w mu`mkin yemes. Woni’n` ushi’n usi’ informaciyani’ qabi’llawshi’ shaxs yekinshi giltten paydalanadi’, bul gilt bolsa si’r saqlanadi’.

Mi’sali’, kompaniya klientleri menen islesiw ushi’n 2 gilt jaratadi’: ashi’q (ha`mmege tarqati’ladi’, mi’sali’, kompaniyani’n` serveri arqali’) ha`m jabi’q (jeke). Bul giltler bir gilttin` yeki bo`legi dep qaralsa boladi’. Klient kompaniyag`a jiberiletug`i’n buyi’rtpasi’ndag`i’ mag`li’wmatlardi’ ashi’q gilt penen kodlaydi’, sonnan keyin woni’ tek g`ana kompaniyani’n` belgili xi’zmetkerleri (si’rli’ gilt penen) woqi’y aladi’. Ha`tteki avtordi’n` wo`zi xabar mazmuni’n bilse de bul shifrlang`an xabardi’ woqi’y almaydi’. Yegerde kompaniya klientke buyi’rtpa, to`lemler xaqqi’ndag`i’ kvitanciyani’ jollamaqshi’ bolsa, wonda woni’ wo`zindegi jabi’q gilt penen kodlaydi’. Klient woni’ ashi’q gilt penen woqi’y aladi’ ha`m soni’n` menen birge bul usi’ xabardi’ sol kompaniyani’n` wo`zi jibergenliginin` da`lili boladi’

Komp`yuter ja`rdeminde shifrlaw algoritmleri

Komp`yuter programmalari’ ja`rdeminde shifrlawshi’ bir qansha algoritmler islep shi’g`i’lg`an. Wolardi’n` ishinde to`mendegi programmalar yen` ken` tarqalg`an:

- Data Ensryption Standart (DES) - simmetriyali’q shifrlaw algoritmi boli’p, AQSh ma`mleketlik standarti’ yesaplanadi’;

- RSA - ashi’q giltli shifrlaw algoritmi (asimmetriyali’q) boli’p, woni’n` ati’ jarati’wshi’lardi’n` ati’ni’n` bas ha`riplerinen ali’ng`an (Rivest, Shamir, Adlleman);
- GOST 28147-89 - simmetriyali’q shifrlaw algoritmi boli’p, ol SSSRda, keyinshelik Rossiyada ma`mleketlik standart si’pati’nda qabi’llang`an.

Absolyut shi’damli’ (turaqli’) shifr

Shennon teoremasi’. Absolyut shi’damli’ shifrlar bar, yag`ni’y sonday shifrlar, wolardi’ sheksiz waqi’t ha`m sheksiz yesaplaw resurslari’na iye bolg`anda da ashi’w mu`mkin yemes.

Shennon shifrdi’n` absolyut shi’damli’ boli’wi’ ushi’n shifrlaw algoritminde qollanatugi’n informaciya ko`lemi shifrlanatug`i’n xabardag`i’ informaciya ko`leminen kem bolmawi’ kerek degen. *Shifrdi’n` si’rli’li’g`i’ shifrlaw algoritmi yemes, ba`lki gilt si’rli’li’g`i’ arqali’ ta`miyinlenedi.*

Simmetriyali’q usi’llarda shifrlawda qollani’latug`i’n gilt $\boldsymbol{K}$ arqali’ joqari’dag`i’ ten`lemelerdi to`mendegishe jazami’z:

$\boldsymbol{T'} = \boldsymbol{E_K}(\boldsymbol{T})$ (shifrlaw),

$\boldsymbol{T} = \boldsymbol{D_K}(\boldsymbol{T'})$ (deshifrlaw).

Deshifrlawda to`mendegi ten`leme wori’nli’: $\boldsymbol{E_K}(\boldsymbol{D_K}(\boldsymbol{T})) = \boldsymbol{T}$.

Kriptograiyani’n` rawajlani’wi’nda yen` a`hmiyetli boli’p K.Shennonni’n` absolyut turaqli’ shifr bar ha`m wol jalg`i’z yekenligi haqqi’ndag`i’ alg`an na`tiyjeleri boldi’. Bunday (jalg`i’z absolyut turaqli’) shifr boli’p ashi’q teksti sonday uzi’nli’qtag`i’ pu`tkilley tosi’nanli’ gilt penen birlestirilgen tek bir ret qollani’latug`i’n lenta xi’zmet yetiwi mu`mkin.

Absolyut turaqli’ shifrdi’n` du`zilisin ha`m qollani’w mumkinshiliklerin ko`rip shi’g`ami’z. Bunday shifrdi’n` a`meliyatta ken` tarqalg`an ha`m a`piwayi’

tu`ri – bul Vernamni’n` shifri’ boli’p, wol n-bitli’ ashi’q tekstti bitpe-bit n-bitli’ gilt penen qosi’wdi’ a`melge asi’radi’.

$$y_i = x_i \oplus k_i, \quad i = 1, \ldots, n.$$

Bunda $x_1 \ldots x_n$ – ashi’q tekst, $k_1, \ldots, k_n$ - gilt, $y_1 \ldots y_n$ – shifrlang`an tekst.

Ja`nede ayti’p ketiwimiz kerek, shifrdi’n` absolyut turaqli’ boli’wi’ ushi’n bir retlik lentag`a qoyi’latug`i’n to`mendegi sha`rtlerdin` ha`r biri wori’nlani’wi’ za`ru`r

- gilttin` pu`tkilley tosi’nanli’ boli’wi’, bul degenimiz giltti qanday da bir quri’lmada jarati’w mu`mkin yemes;
- gilt uzi’nli’g`i’ ashi’q tekst uzi’nli’g`i’na ten` boli’wi’ kerek;
- giltten tek bir ret paydalani’ladi’

Usi’ sha`rtlerdin` keminde birewi buzi’lg`anda shifr absolyut turaqli’ bolmay qaladi’ ha`m woni’ buzi’w mu`mkinshiligi (a`melge asi’ri’w qansha qi’yi’n bolsa da) payda boladi’. Biraq tap sol sha`rtler absolyut turaqli’ shifrdi’ ju`de qi’mbat ha`m a`meliy jaqtan qolaysi’z yetedi. Bunday shifrdan paydalani’w ushi’n biz barli’q abonentlerdi jeterli da`rejede tosi’nanli’ giltler toplami’ menen ta`miynlewimiz ha`m wolardan qayta paydalandi’rmawi’mi’z kerek boladi’. Buni’ a`melge asi’ri’w ju`de qi’mbat ha`m qi’yi’n.

Joqari’da keltirilgen sebeplerden absolyut turaqli’ shifrlar tek uzati’li’p ati’rg`an informaciya ko`lemi kishi bolg`an baylani’s tarmaqlari’nda qollani’ladi’. A`dette bul joqari’ da`rejede si’rli’ bolg`an ma`mleketlik informaciyani’ uzati’w tarmaqlari’ boli’p tabi’ladi’.

Absolyut turaqli’ shifr (Vernam)

Joqari'da ayti'lg`anday, absolyut turaqli' shifrlardi'n` sekreti gilt K arqali' ani'qlanadi'. Shennonni'n` giltlerge qoyg`an talabi': gilttin` wo`lshemi shifrlani'p ati'rg`an teksttin` wo`lsheminen kishi bolmawi' kerek, yag`ni'y $|K| \geq |T|$. Meyli, wolardi'q wo`lshemi birdey $N$ bit bolsi'n: $|K| = |T| = N$. Bul shifr absolyut turaqli' boli'wi' mumkin ushi'n minimum. Shifrlaw ushi'n tekst (xabar) $T$ gilt $K$ menen belgili bir binar woperaciya $\circ$ ja`rdeminde sonday kombinaciya yetiliwi kerek, woni'n` na`tijesinde payda bolg`an shifrotekst bir waqi'tti'n` wo`zinde da`slepki tekst T ha`m gilt $K$ –g`a g`arezli bolsi'n.

Bunda shifrlaw ten`lemesi to`mendegi ko`riniste boladi':

$$T' = E_K(T) = T \circ K.$$

Shifrlang`an teksttin` wo`lshemi de $N$ bit-ke ten` boladi': $|T'| = |T| = |K| = N$. Shifrdi'n` absolyut turaqli'li'gi'n ta`miynlew ushi'n gilt K-dag`i' si'rli' informaciya ko`lemi woni'n` ko`lemi ushi'n mu`mkin bolg`ansha yen` maksimal boli'wi' kerek. Bul degenimiz, gilttin` barli'q bitleri tosi'nanli', ma`nisleri ten` itimalli' ha`m statistikali'q g`arezsiz boli'wi' sha`rt. Bunday sha`rtke juwap beretug`i'n gilt algoritmlik jol menen tabi'lmaydi', bunda tek apparatli'q usi'ldan paydalanami'z.

Yendi operaciya $\circ$ -g`a qoyi'latug`i'n talaplardi' ko`rip shi'g`ami'z. Birinshiden, shifrlaw menen birge deshifrlaw ha`m mu`mkin boli'wi' ushi'n ten`leme $T \circ K = T'$ qalegen $T'$ ha`m K ushi'n bir sheshimge iye boli'wi' kerek. Demek, binar operaciya $\circ$ ushi'n keri operaciyabar boli'wi' kerek, woni' $\bullet$ dep belgileymiz. Soni'n` menen birge berilgenlerdin` qalegen N-bitli' bloklari' T ha`m $K$ ushi'n ba`rhama to`mendegi ten`lik wori'nli' $(T \circ K) \bullet K = T$. Yekinshiden, shifrdi'n` toli'q si'rli' boli'wi'n ta`miynlew ushi'n ha`r tu`rli giltler birdey da`slepki tekstler ushi'n ha`r tu`rli shifrtekst beriwi sha`rt. Bul talap ten`leme $T \circ K = T'$ K arqali' tek bir sheshimge iye boli'wi'n talap yetiw menen birdey.

Shifrlang`an xabardi'n` si'rli'li'g`i' tikkeley gilttin` si'rli'li'g`i' menen ani'qlani'wi'na baylani'sli' bolg`anli'qtan, qalg`an jag`i'nan operaciyalar ∘ ha`m • qalegenshe, wo`zin`izge qolayli' yetip, tan`lani'wi' mumkin. Bunday operaciyalar si'pati'nda modul` $2^N$ boyi'nsha qosi'w ha`m ayi'ri'w operaciyasi' tan`lani'wi' mu'mkin

$$T \circ K = (T + K) \bmod 2^N, \quad T \bullet K = (T - K) \bmod 2^N.$$

Pu`tin bir xabardi'n` u`stinde, woni'n` uzi'nli'g`i' sebepli, yesaplawlar ju`rgiziw qi'yi'nshi'li'q tuwdi'ri'wi' mu`mkin. Sol sebepli xabardi' ha`m giltti kishi ko`lemli bloklarg`a bo`lgen maqul. Joqari'da ayti'lg`an operaciyalardi' usi' bloklarg`a birme-bir qollanami'z:

$$T = (T_1, T_2, ..., T_n), \quad K = (K_1, K_2, ..., K_n), \; |K_i| = |T_i| = N_i,$$

$$T_i \circ K_i = (T_i + K_i) \bmod 2^{Ni}, \quad T_i \bullet K_i = (T_i - K_i) \bmod 2^{Ni}.$$

Bul procesti aqi'ri'na deyin jetkizsek, wonda biz modul` 2 boyi'nsha bitpe-bit qosi'w operaciyasi'na kelemiz, basqasha bul operaciyani' bitpe-bit yaki shi'g`ari'p taslaw operaciyasi' dep ataladi':

$$T \circ K = T \bullet K = T \oplus K.$$

Yen' son`g`i' operaciya wo`zine keri boli'p shi'qti' ha`m sol sebepli ha`mde a`piwayi' bolg`anli'g`i' ha`m wori'nlaw an`satli'g`i' sebepli (bunda xabardi'n` bo`lek bitleri bir-birinen biyg`arez tu`rde qayta islenedi), yen` ken` tarqalg`an boli'p tabi'ladi'.

Biz ha`zir islep shi'qqan shifr Vernamni'n` bir ret qollani'latug`i'n gammasi' dep ataladi'. Bul shifr absolyut turaq boli'p tabi'ladi', biraq wol qi'mbatqa tu`sedi, sebebi xabardi' shifrlaw ushi'n bunda sol uzi'nli'qtag`i' gilt ha`m xabardi' jo`netiwshige, ha`m woni' qabi'llawshi'g`a jetkerip beriliwi tiyis.

Yeki tu`r xabardi' shifrlaw ushi'n birdey gamma elementlerinin` izbe=izligin qollani'wg`a bolmaydi', wolardi'n` ha`r birine izbe-izlik bo`lek islep shi'g`i'ladi'.

Yegerde bul talap buzi'lg`an bolsa, wonda ba`rhama ⊗ ha`m ∅ binarli'q operaciyalari'ni'n` sonday jupli'g`i'n tabi'wg`a boladi', wolardi' berilgenler gammasi'ni'n` birdey elementin paydalani'p, tiyisli tu`rde ashi'q tekst bloki' ha`m shifrlang`an blokqa qollang`anda, wolar birdey na`tiyje beredi:

$$T_i' \otimes \tilde{T}_i' = T_i \varnothing \tilde{T}_i.$$

Xabarda qansha ko`p arti'qsha mag`li'wmat bolsa, sonshelli kriptoanaliz qi'li'w an`sat boladi'.

Yegerde gammani' qosi'w ushi'n modul` 2 boyi'nsha bitpe-bit qosi'w operaciyasi' paydalani'lsa, wonda na`tijege si'rli' gamma ta`sirin jasi'ri'wshi' binarli'q operaciyalar si'pati'nda sol operaciyani'n` wo`zin qollani'wg`a boladi'. Haqi'yqati'nda-da, meyli yeki blok birdey gamma elementi $\square_i$ ja`rdeminde shifrlansi'n:

$$T_i' = T_i \oplus \square_i,$$

$$\tilde{T}_i' = \tilde{T}_i \oplus \square_i,$$

Yendi shifrtekst bloklari'n modul` 2 boyi'nsha bitpe-bit qosami'z:

$$T_i' \oplus \tilde{T}_i' = (T_i \oplus \square_i) \oplus (\tilde{T}_i \oplus \square_i) = (T_i \oplus \tilde{T}_i) \oplus (\square_i \oplus \square_i) = (T_i \oplus \tilde{T}_i) \oplus 0 = T_i \oplus \tilde{T}_i.$$

Ali'ng`an na`tije ashi'q tekst bloklari'ni'n` modul` 2 boyi'nsha bitpe-bit qosi'ndi'si' menen birdey, bul degenimiz kriptoanalikke hesh qanday jumi's qalmadi'.

Ha`r bir shifrlanatug`i'n xabar ushi'n wo`zinin` unikal gammasi'n jarati'w talabi' Vernam usi'li' menen xabarlardi' shifrlaw jumi'slari'n ju`de qi'mbatqa tu`siredi. Bul usi'ldan paydalani'w ekonomikali'q jaqtan tek g`ana joqari' da`rejede a`hmiyetli xabarlardi' baylani's kanallari' arqali' uzati'wda ha`m siyrek paydalang`anda wo`zin aqlaydi'.

Simmetriyali'q giltli algoritmler klassi'na "bir ret qollani'latug`i'n bloknot" [one-time pad] metodi' kiredi. Bul algoritm shifrlanatug`i'n tekstti bitpe-bit gilt

boli’p xi’zmet yetetug`i’n tosi’nanli’ bitler izbe-izligi menen qosi’p baradi’ (gammalaydi’).Bunda gilttin` uzi’nli’g`i’ shifrlanatug`i’n teksttin` uzi’nli’g`i’ menen birdey boli’wi’ kerek. Soni’n` menen birge gilttin` ha`r bir bo`legi tek bir ret paydalani’wi’ mu`mkin; keri jag`dayda tekst an`sat deshifrlanadi’. Usi’ sha`rtler wori’nlang`anda bul metod teoriyada buzi’lmaytug`i’n jalg`i’z usi’l boli’p tabi’ladi’.

***"Ryukzak problemasi’" tiykari’ndag`i’ algoritm.*** "Ryukzak problemasi’" to`mendegishe ta`riyplenedi.

Natural sanlar ko`pligi A = (a1,a2,..., an) ha`m natural san S berilgen bolsi’n. Bizden elementlerinin` qosi’ndi’si’ S bolg`an A ko`pliginin` u`les ko`pligi barli’g`i’n ani’qlaw talap yetiledi.

Yag`ni’y: (0,1) intervali’nda sonday xi (i<=n) bar ma, wol ushi’n Σai *xi = S (1<=i<=n) ?

Bul problemani’ basqasha ta`riyplew ha`m mu`mkin. Awi’rli’qlari’ belgili bolg`an bir neshe zatlar ko`pligi ha`m bir ryukzak bar bolsi’n. Ryukzakti’n` ishine sali’natug`i’n zatlardi’n` uli’wma awi’rli’g`i’ berilgen ma`nisten aspawi’ kerek.

Ryukzakqa sali’natug`i’n zatlar toplami’n sonday qi’li’p tan`law mu`mkin be, wolardi’n` awi’rli’g`i’ mu`mkinshiligi bari’nsha da`l maksimal bolsi’n?

"Ryukzak problemasi’ " quramali’ boli’p esaplanadi’ ha`m woni’n` sheshimi ha`zirgeshe tabi’lmag`an.

***Ryukzak problemasi’ tiykari’nda shifrlaw sistemasi’n du`ziw*** ideyasi’ni’n` mazmuni’ ryukzakti’ toldi’ri’w ma`selesinin` belgili bir sheshiliwi an`sat bolg`an bo`legin (podklass) aji’rati’p ali’w ha`m bul klasstag`i’ ma`selelerdi belgili bir wo`zgertiwler ja`rdeminde uli’wma klassqa uqsas yetip "maskirovka yetiw" boli’p

tabi’ladi’. Bul u`les klass parametrleri jasi’ri’n giltti, al modifikaciya etilgen ma`sele parametrleri ashi’q giltti ani’qlaydi’.

An`sat sheshiletug`i’n ma`sele si’pati’nda R. Merkl` ha`m M. Xellman 1978 j. "super wo`siwshi" ryukzakti’ tolti’ri’w ma`selesin usi’ng`an. Woni’n` ma`nisi to`mendegishe.

Super wo`siwshi dep sonday (b1,b2,..., bn ) natural sanlar izbe-izligine aytami’z, wol to`mendegi qa`siyetlerge iye bolsi’n: bi>Σbj , 1<=j<=i-1 , 2<i<n .

Super wo`siwshi izbe-izlik ushi’n ryukzak problemasi’ to`mendegi adi’mlardi’ wori’nlaw procedurasi’ ja`rdeminde sheshiliwi mu`mkinligin tekseriwge boladi’:

1. i = n dep ali’w;

2. Yegerde i>1 bolsa, wonda xi ten` 1 dep ha`m yegerde S>bi bolsa, Sten` S – bi dep,

ha`m keri jag`dayda xi ten` 0 dep alami’z;

3. i ten` i–1 dep ali’p, 2-shi adi’mg`a qayti’w.

Ryukzak problemasi’na tiykarlang`an sistemada S ma`nisi sistemani’n` parametri boli’p tabi’ladi’.Ashi’q ha`m jasi’ri’n giltlerdi yesaplaw ushi’n sistemani’n` ha`r bir abonenti to`mendegi a`meller izbe-izligin wori’nlaydi’.

1. Super wo`siwshi (b1, b2,..., bn) izbe-izligin ha`m sonday modul` m tan`laydi’, wonda m>Σbi , 1<=i<=n .

2. Tosi’nanli’ san W sonday yetip tan`lanadi’, bunda 1<W<m-1, NOD(W,m) =1 wori’nli’ bolsi’n.

3. (1, 2,...,n) sanlari'ni'n` tosi'nanli' worni'n almasti'ri'w izbe-izligin π tan`laydi'.

4. i=1…n ushi'n ai =(W* bπ(i)) mod (n) yesaplaydi'.

Ashi'q gilt boli'p (a1 ,a2,...,an) toplami', al jasi'ri'n gilt boli'p – (π, m, W, (b1, b2,…,bn)) toplami' xi'zmet yetedi.

Abonent A ushi'n arnalg`an M xabari'n shifrlaw ushi'n abonent V abonent A-ni'n` ashi'q gilti bolg`an (a1,a2,...,an) ja`rdeminde to`mendegi adi'mlardi' wori'nlaydi':

1. Xabar M uzi'nli'g`i' n bolg`an binar izbe-izlik M =M1M2 ...Mn tu`rge keltiriledi;

2. S =Σ Mi *ai , i=1…n yesaplaydi' ha`m woni' A-g`a jiberedi .

Abonent A xabar S qabi'llag`annan keyin, N = (W-1 *C ) mod (m) yesaplaydi', keyin bolsa, super wo`siwshi izbe-izlik ushi'n ryukzak problemasi'n sheship, sonday sanlar zi , i = (0,1) tabadi', bunda H=Σzi*bi , (i=1,…,n) wori'nlanadi'.

Mi izbe-izliginin` bitleri to`mendegi formula menen yesaplanadi':

$$Mi=z\pi(i),\ i=1,\ldots,n.$$

Joqari'dag`i' deshifrlaw procedurasi'ni'n` korrektligi to`mendegi pikirlewlerden kelip shi'g`adi'.

$$H=W\text{-}1*C=W\text{-}1*\Sigma Mi*ai = (\Sigma\ Mi*b\pi(i))\ (\mathrm{mod}\ m)$$

ha`m 0<H<m boli'wi' sebepli , H=Σ Mi*bπ(i) , (i=1,…,n), ha`m, demek, ryukzak problemasi'n sheshiw algoritmi xaqi'yqati'nda da ashi'q teksttin` wori'nlardi' almasti'ri'w π arqali' almasti'ri'lg`an bitlerin tabadi'.

RSA algoritmi

RSA (1977j., ati' avtorlari' Rivest, Shamir, Adleman atlari'nan kelip shi'qqan) algoritmi asimmetriyali'q (ashi'q giltli) kriptosistemalarda ken` qollani'ladi'.

Bul algoritmnin` tiykari'nda to`mendegi fakt jatadi'. Ulken a`piwayi' sanlardi' tabi'w an`sat, biraq bunday yeki sanni'n` ko`beymesin a`piwayi' ko`beytiwshilerge bo`liw (jayi'w) mu`mkin yemes.

RSA shifri'n ashi'w usi'nday jayi'w a`meline ekvivalent yekenligi da`liyllengen. Sol sebepli qalegen uzi'nli'tag`i' gilt ushi'n bul shifrdi' ashi'wg`a ketetug`i'n operaciyalar sani'ni'n` to`mengi bahasi'n beriw mu`mkin, al ha`zirgi zaman komp`yuterlerinin` wo`nimdarli'g`i'n yesapqa ali'p woni'n` ushi'n ketetug`i'n waqi'tti' bahalaw da mu`mkin. RSA algoritminin` basqalardan ayri'qshali'g`i' da sonda, yag`ni'y biz bul algoritmnin` qorg`alg`anli'q da`rejesin ani'q bahalay alami'z.

Algoritm a`piuayi' sanlardi'n` matematikali'q qasiyetlerine tiykarlang`an.

Bunda yeki a`piwayi' san tan`lanadi': *r ha`m q*. Keyin wolardi'n` ja`rdeminde ja`ne u`sh san tan`lanadi' :

- *p - r ha`m q* ko`beymesi*;*
- *d* —bul (r-1) ha`m (d-1) sanlari'ni'n` ko`beymesi menen wo`z ara a`piwayi' bolg`an san;
- *e* –sonday san, *(e*d)(mod* ((r-1)(d-1))) – a`piwayi' san boladi'.

Yendi alfavitti cifrli' tu`rde beremiz *(A→1, B → 2*, h.t.b.) ha`m xabardi' mi'na formula ja`rdeminde shifrlaymi'z:

$$x_i = u_i^{\,e} (mod\ n),$$

bunda x_i — shifrlang`an teksttin` gezektegi ha`ripi, $u_i$ - ashi'q teksttin` gezektegi ha`ripi.

Deshifrlaw da sol formula ja`rdeminde a`melge asi'ri'ladi', tek *e* –ni'n` worni'na *d* qoyi'ladi', al *x* penen *u w*ori'n almasadi'.

Jupli’q *{e, p}* — ashi’q gilt dep ataladi’ ha`m ashi’qtan ashi’q ja`riyalanadi’, wodan qalegen adam paydalani’wi’ mu`mkin, al jupli’q *{d, p}*-jabi’q gilt boli’p tabi’ladi’ ha`m adresatda saqlanadi’.

Mi’sal. Meyli, da`slepki xabar "CAB" bolsi’n. A`dette u`lken sanlar tan`lanadi’, biraq biz jumi’si’mi’zdi’ an`satlasti’ri’p, kishi sanlar menen islesemiz

1. Demek *r=3 ha`m* g= 11 dep alami’z

2. n=3*11=33 boladi’

3. (r-1)(d-1)=20 boladi’. Demek, *d* si’pati’nda 20 menen a`piwayi’ bolg`an sandi’ alami’z, mi’sali’, *d=3.*

4. Yendi *e* sani’n tan`laymi’z. Bunday san si’pati’nda *(e*d) (mod((r-1)(d-1))) =1*, yag`ni’y *(e*3)* (mod 20) = 1 qanaatlandi’ratug`i’n qalegen sandi’ alami’z, mi’sali’ 7.

5. Shifrlanatug`i’n xabardi’ A→1, B → 2, S →3 sa`wlelendiriw ja`rdeminde pu`tin sanlar izbe-izligi tu`rde beremiz. Sonda xabar SAV → (3,1,2) ko`rinisinde boladi’. Endi oni’ {7,33}gilti ja`rdeminde shifrlaymi’z.

$x_1 = (Z^7) \pmod{33} = 2187 \pmod{33} = 9,$

$$x_2 = (I^7) \pmod{33} = 1 \pmod{33} = 1,$$

$x_3 = (2^7) \pmod{33} = 128 \pmod{33} = 29.$

6. Shifrlang`an (9,1,29) xabardi’ jabi’q gilt {3,33}ja`rdeminde deshifrlaymi’z:

$$y_1 = (9^3) \pmod{33} = 729 \pmod{33} = 3,$$

$$y_2 = (I^3) \pmod{33} = 1 \pmod{33} = 1,$$

$$u_3 = (29^3) \pmod{33} = 24389 \pmod{33} = 2.$$

Giltlerdi bo`listiriw (Diffi-Xellman) sistemasi’

Da`stu`riy kriptografiyali’q sistemalarda paydalani’wshi’lardi’n` ha`r bir jupli’g`i’ xabarlari’n shifrlawda ha`m deshifrlawda jalg`i’z bir jasi’ri’n giltten paydalanadi’. Bunda bir paydalani’wshi’dan yekinshisine giltti uzati’wdi’n` isenimli joli’n tabi’w kerek boladi’.

Yegerde paydalani’wshi’lar giltti tez-tezden almasti’ri’p tursa, wonda woni’ paydalani’wshi’larg`a jetkeriw u`lken mashqalag`a aylanadi’. Wonnan qalsa, da`stu`riy kriptosistemalarda jan`a paydalani’wshi’g`a isenimli baylani’s kanali’ arqali’ giltti jibermegenshe wog`an xabardi’n` wo`zin de jiberiw mu`mkin yemes. Bul mashqalani’n` sheshimi ashi’q giltlerdi bo`listiriw sistemasi’n (public-key distribution system) jarati’w arqali’ tabi’ldi’. Bul sistemada qorg`almag`an baylani’s kanallari’ arqali’ paydalani’wshi’lar wo`zlerinin` si’rli’ giltleri menen almasi’wi’ mu`mkin.

Birinshi bunday sistema boli’p Diffi-Xellman sistemasi’ (1976j.) tabi’ladi’ ha`m wol diskretli logarifmlestiriw ma`selesi tiykari’nda jarati’lg`an. Aytayi’q, yeki paydalani’wshi’ A ha`m V bir-biri menen baylani’spaqshi’. Bul degeni, wolar gilt **K** tuwrali’ bir kelisimge keliwi kerek**.**

Diffi-Xellman sistemasi’nda qalay gilt almasi’ladi’?

Meyli N – bir u`lken pu`tin san bolsi’n, al G – basqa bir pu`tin san, 1 <= G <= N-1.

Giltler almasi’w procedurasi’n adi’m ba adi’m ko`rip shi’g`ami’z

1. Da`slep A ha`m V N ha`m G ma`nisleri boyi’nsha bir kelisimge keledi (a`dette, bul ma`nisler sistemani’n` barli’q paydalani’wshi’lari’ ushi’n standart, yag`ni’y birdey boladi’).
2. Keyin A bir u`lken pu`tin san X tan`laydi’ ha`m to`mendegini esaplaydi’

X_x = G^X MOD N.

Wo’z gezeginde V Y sani’n tan`laydi’ ha`m

Y_y = G^Y MOD N

yesaplaydi’.

Keyin bolsa A ha`m V bir biri menen $X_x$ ha`m Y_y ma`nislerin almasadi’. (Bunda biz uzati’li’p ati’rg`an mag`li’wmatlar jawi’z nietli shaxs ta`repinen qolg`a kiritiliwi mu`mkin dep yesaplaymi’z). X ha`m Y sanlari’n A ha`m V si’r saqlaydi’.

3. V –dan Y_y sani’n alg`annan keyin, A

K(1) = Y_y^X MOD N

ma`nisin, al V bolsa

K(2) = X_x^Y MOD N yesaplaydi’.

Biraq,

Y_y^X MOD N = G^(X*Y) MOD N = X_x^Y MOD N, demek,

K(1) = K(2) = K.

Tabi'lg`an K ma`nisi shifrlaw giltinin` da`l wo`zi boladi'.

Al jawi'z nietli shaxs ne isleydi? Woni'n` qoli'na da G, N, $X_x$ ha`m Y_y kelip tu`sken, yendi wol K giltin tabi'w kerek. Bul ma`seleni sheshiwdin` yen` a`piwayi' usi'li' boli'p G, N, $X_x$ ma`nisleri boyi'nsha X tabi'w, yaki hesh bolmag`anda sonday X' tabi'w kerek,

G^X' MOD N = X

wori'nli' bolsi'n, sebebi bul jag`dayda

Y_y^X' MOD N = K.

Biraq bul ma`sele diskretli logarifmlestiriw ma`selesi boli'p tabi'ladi' ha`m wol sheshilmeytug`i'n boli'p yesaplanadi'.

Diffi-Xellman sistemasi' yeki paydalani'wshi'g`a bir si'rli' gilt tuwrali' kelisimge keliw mu`mkinshiligin beredi. Biraq bul sistema keyinshelik informaciya qalay shifrlani'wi'na hesh qanday ta`sir yete almaydi'. Bul degeni, yegerde A V-ga wo`zinin` jasi'ri'n M xabari'n jibermekshi bolsa, wonda Diffi-Xellman arqali' gilt ani'qlang`annan keyin shifrlawdi'n` qalegen sistemasi'nan paydalani'w mu`mkin.

Biraq ashi'q giltli sistemalar tek g`ana giltlerdi bo`listiriw ma`selesin sheshiw ushi'n jarati'lmag`an. Kerek bolsa bul sistemadan informaciyani' shifrlawda da effektiv turde paydalani'w mu`mkin. Sebebi, ani'qlamasi' boyi'nsha, ashi'q giltli sistemani'n` ayri'qshali'g`i' sonda, shifrlaw giltin bilgen adam tekstti deshifrlawdi' shekli waqi't ishinde a`melge asi'ra almaydi'. Buni' ko`rip shi'g`ayi'q.

Paydalani'wshi' A yeki algoritmge iye: E – xabardi' shifrlaw ha`m D – deshifrlaw ushi'n. Algoritm E ashi'q ja`riyalanadi', mi'sali' giltler katalogi' arqali', al algoritm D si'r saqlanadi'. Yegerde V yaki jawi'z nietli shaxs A-g`a xabar jibermekshi bolsa, wol giltler katalogi'nan algoritm E-ni izlep tabadi' ha`m xabardi' shifrlawda paydalanadi'. Biraq, wol xabardi' tek g`ana A deshifrlay aladi', sebebi tek wol algoritm D-g`a iye. Demek, E ha`m D to`mendegi sha`rtke bag`i'ni'wi' kerek:

D(E(M)) = M, qalegen xabar M ushi'n

Demek, E algoritmin biliw (xabardi' jasi'ri'w) D-ni' a`melge asi'ri'w (xabardi' ashi'w) ushi'n jetkilikli yemes.

El-Gamal algoritmi

Ashi'q giltli kriptosistemalarda ken`nen bir ta`repleme funkciya ideyasi' kollani'ladi'. Yag`ni'y berilgen argument *x* boyi'nsha *f(x)* yesaplaw mu`mkin, biraq belgili *f(x)* boyi'nsha *x* tabi'w qi'yi'nshi'li'q tuwdi'radi'.

El-Gamal algoritmi (1985 j.islep shi'g`i'lg`an, avtori' El`-Gamal`) AQSh –ta cifrli' imza standarti'nda (Digital Signature Standard) isletiledi.

Bul metodti'n` RSA algoritminen ayi'rmashi'li'g`i' El`-Gamal`di'n` metodi' diskret logarifm mashqalasi'na tiykarlang`anli'g`i'nda. Woni'n` ma`nisi, shekli maydanda sandi' da`rejege ko`teriw an`sat, biraq woni'n` ma`nisi arqali' argumentti tabi'w, yag`ni'y logarifmdi tabi'w qi'yi'nshi'li'q tuwdi'radi'.

Sistemani'n` tiykari'nda *p ha`m g* parametrleri jatadi', bunda *p* - a`piwayi', al *g* – pu`tin san. Paydalani'wshi' A jasi'ri'n gilt *a* generaciya yetedi ha`m ashi'q giltti yesaplap tabadi'

$$u = g^a \bmod p.$$

Bunda *u, p* ha`m *g* – ashi'q gilt boladi'. Bir toparg`a kiriwshi paydalani'wshi'lar ushi'n *p* ha`m *g* ma`nislerin birdey yetip qabi'llaw mu`mkin. Jabi'k gilt boli'p bolsa *a* ma`nisi xi'zmet yetedi.

El Gamal usi'li' elektron imza jarati'wda qollani'li'wi' mu`mkin.

Yegerde Paydalani'wshi' V paydalani'wshi' A-g`a xabar *t* jibermekshi bolsa, wonda wol *r* dan kishi bolg`an tosi'nanli' san *k*,tan`laydi' ( *k, ha`m (p-1)* – wo`z ara a`piwayi').

$u_1 = g^k \bmod r$ *ha`m* $u_2 = t \oplus u$, bunda $\oplus$ - modul` 2 boyi'nsha bit-pe-bit qosi'w. Keyin Paydalani'wshi' V jupli'q (u_1,u_2)-ni' (imza) Paydalani'wshi' A-g`a jiberedi.

Paydalani'wshi' A shifrlang`an xabardi' ali'p, woni' qayta tikleydi

$$m = (y'' \bmod p) \oplus y_2$$

Modul` 2 boyi'nsha bitlerdi qosi'w a`meli

Bul a`mel S programmalasti'ri'w tilinde ^ belgisi menen, matematikada bolsa + belgisi menen belgilenedi ha`m bitler u`stinde to`mendegi standart logikali'q a`meldi ori'nlaydi':

0+0=0
0+1=1
1+0=1
1+1=0

Modul` 2 boyi'nsha qosi'w a`meli ja`rdeminde ashi'q tekstti shifrlaw mu`mkin. Woni'n` ushi'n ashi'q teksttin` ha`r bir biti gilttin` ha`r bir biti menen modul` 2 tiykari'nda qosi'ladi'. Na`tijede shifr teksti payda boladi'. Qayta ashi'w ushi'n bolsa ja`ne sonday qag`i'yda boyi'nsha shifr teksti ha`m gilt kosi'ladi'. Na`tijede ashi'q tekst payda boladi'. Bul shifrlaw usi'li' simmetriyali'q shifrlaw yesaplanadi'.

El Gamal usi'li'n elektron imza jarati'wda qollani'w

Xabar m –g`a imza qoyi'w ushi'n (p-1) menen a`piwayi' bolg`an tosi'nanli' *k* tan`lanadi' ha`m

$y_1=g^k \ mod \ p$ yesaplanadi'.

Keyin Evklid algoritminin` ken`eytirilgen tu`rinen paydalani'p to`mendegi ten`lemeden y_2 tabi'ladi'

$$m = (ay_1+ky_2) \bmod (p-1)$$

Elektron imza boli'p y_1 *ha`m* $y_2$ jupli'g`i' xi'zmet yetedi. Tosi'nanli' san *k* si'r saqlanadi'. Imzani'n` xaqi'yqi'yli'g`i'n tekseriw ushi'n

$$y^{Y1} \ y_1^{y2} \bmod p = g^m \bmod p$$

xaqi'yqi'y yekenligin tekseriwimiz kerek boladi'.

Metod ha`r bir xabar ushi'n jan`a (tosi'nanli') *k* tan`lawdi' talap yetedi. Bul sistema RSA –ge al`ternativ boli'p yesaplanadi' ha`m giltlerinin` uzi'nli'g`i' ten` bolg`an jag`dayda birdey kriptoturaqli'li'qti' ta`miynleydi.

Mi'sali', p=11, g=2, al jabi'q gilt $a = 8$ dep alami'z. Yendi

$Y_1 = g^a \bmod p = 2^8 \bmod 11=3$ yesaplaymi'z.

Ashi'q gilt boli'p y=3, g=2 ha`m p=11 xi'zmet qi'ladi'. Xabar m=5 bolsi'n, wog`an imza qoyi'w ushi'n tosi'nanli' k =9 tan`laymi'z ha`m mod (9,10)=1 yekenligin tekseremiz. Yendi yesaplaymi'z

$$Y_1 = g^k \bmod p = 2^9 \bmod 11 = 6$$

Ken`eytirilgen Evklid algoritmi ja`rdeminde y_2 tabami'z

$$M = (ay_1 + k\, y_2) \bmod (p-1)$$

$$5 = (8*6+9*y_2) \bmod 10$$

Sheshimi $y_2 = 3$, imza boli'p jupli'q $y_1 = 6$ ha`m $y_2 = 3$ xi'zmet yetedi.

Imzani'n` haqi'yqi'yli'g`i'n to`mendegi an`latpalar

$$y^{Y1}\, y_1^{y2} \bmod p = g^m \bmod p$$

yag`ni'y

$$3^6\, 6^3 \bmod 11 = 2^5 \bmod 11$$

wori'nli' yekenliginen bilemiz.

Yegerde biz bank xi'zmetlerinen paydalani'w ushi'n wo`zimizdin` elektron imzami'zdi' jarati'wi'mi'z kerek bolsa, wonda bank bizden arnawli' programmadan paydalani'p yeki gilt (jabi'q ha`m ashi'q) do`retiwimizdi soraydi'. Ashi'q gilt bankqa beriledi. Mi'sali', biz bankqa r/scheti'mi'z benen islenetug`i'n operaciyalar haqqi'ndag`i' buyi'rtpani' jiberiwde wni' bankti'n` ashi'q gilti menen kodlaymi'z, al asti'na qoyi'latug`i'n imzami'zdi' wo`zimizdin` jabi'q giltimiz benen kodlaymi'z. Bank bolsa keri operaciyani' wori'nlaydi'. Wol buyi'rtpani' wo`zinin` jabi'q gilti menen, imzami'zdi' bolsa – klienttin` ashi'q gilti menen woqi'ydi'. Yegerde bank imzani' woqi'y alsa, demek, bul buyi'rtpa da`l sol klienttin wo`zinen kelgen dep, tu`sinedi.

Demek, informaciyag`a ji'nayatshi' ta`repinen hu`jim jasaw mu`mkin yemesligine kepillik beriwshi mexanizmler ha`m metodlardi'n` toplami' wolardan duri's paydalang`an halda informaciyani'n` konfidencialli'g`i'n ha`m pu`tinligin ta`miyinleydi.

3.3. Informaciyani' kriptografiyali'q qorg'aw ma'selesin programmalasti'ri'w arqali' sheshiwdi u'yretiw

Almasti'ri'w shifrlari'

1. ASCII kodi' arqali' shifrlaw

Bul shifrlaw usi'li' da'slepki teksttin' ha'r bir ha'ribin to'mendegishe wo'zgertedi.

Meyli ***x*** –teksttin' bir ha'ribi, al ***x'*** sol ha'riptin' shifrlang'an ko'rinisi, yag'niy shifrlaw procesinde ***x*** ha'ribi ***x'*** ha'ripke almasti'ri'ladi'.

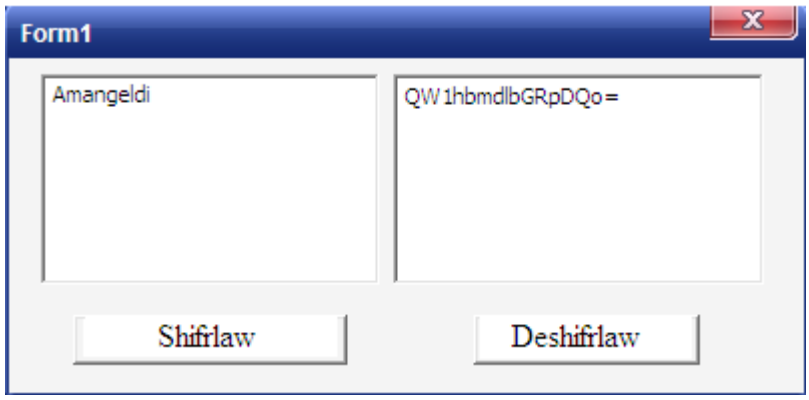
D(x)=x'

N – ***x*** ha'ribinin' ASCII kodi'nda worni', shifrlaw na'tiyjesinde ***x*** ASCII kodi'nda ***N'*** –shi wori'nda turg'an ***x'*** ha'ripke almasti'ri'ladi'.

N'=N+gilt

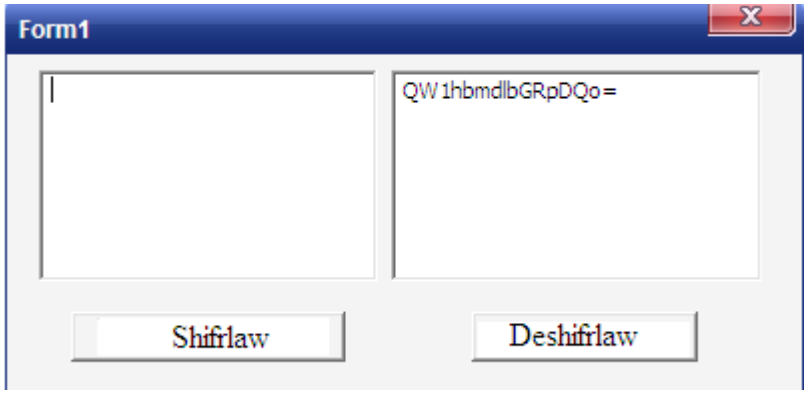
Mi'sali' shifrlaw programmasi' fayli'n ashami'z ha'mde shifrlaw bo'limine kerekli so`zdi jazamız.

Yendi shifrlaw komandasi’n basami’z.

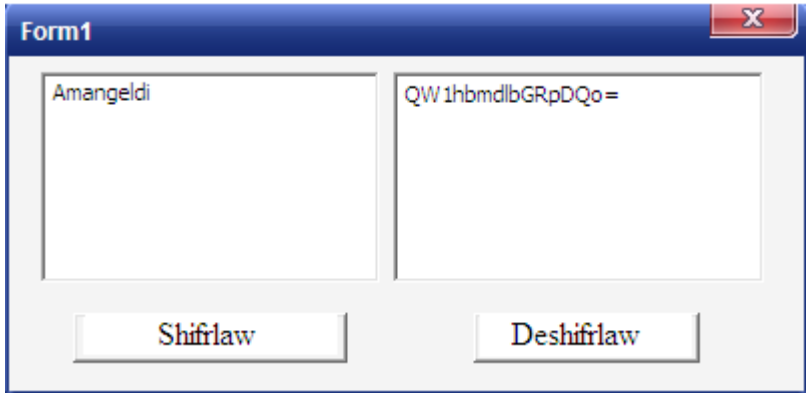


Shifrlaw tabi’sli’ a’melge asi’ri’ldi’.

Yendi bul tekstti qaytadan tikleymiz. Woni’n’ ushi’n Deshifrlaw komandasi’n beremiz.



Deshifrlaw kamandası a’melge asi’ri’lg`annan son` tekstimiz aldıng`ı jag`dayına keledi.



2. Tekstli fayldi’ shifrlaw

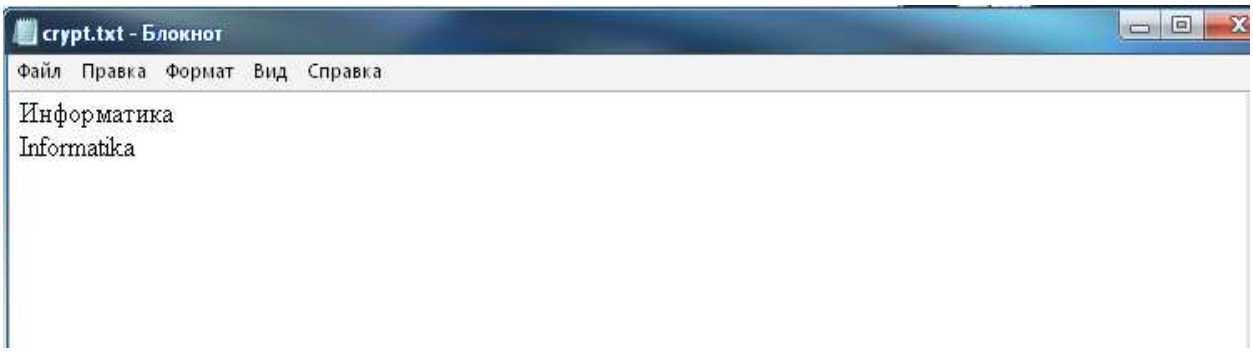
Bul shifrlaw usi’li’nda .txt ken’eytpeli fayl teksti shifrlanadi’.

Formada fayl adresin kiritiw soraladi’. Keyin fayl mazmuni’ ashi’ladi’ ha’m gilt soraladi’. Gilt dep berilgen san tekstti’ neshe ha’ripten bloklarg’a aji’rati’p shifrlawdi’ belgileydi. Ha’r bir bloktag’i’ tekst terisine shfrlanadi’.

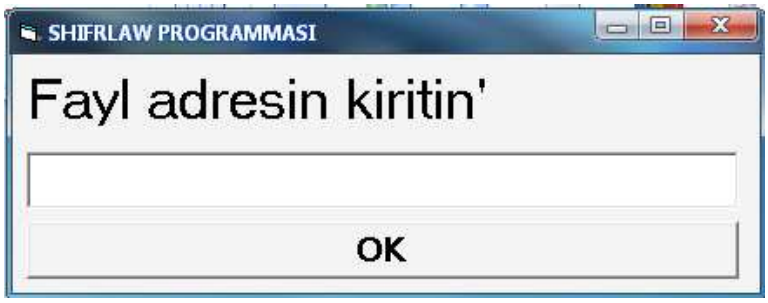
Deshifrlaw da sol jerde a’melge asi’ri’ladi’.

Qi’zi’g’i’ sonda, shifrlag’annan keyin bul tekstli fayl avtomatik tu’rde shifrlang’ani’ boyi’nsha saqlanadi’.

Tekstli fayl mazmuni’



SHIFRLAW PROGRAMMASI.exe fayli’n ashamiz’



Shifrlanatug’i’n fayl adresin kiritemiz (C diskda crypt.txt fayli’)

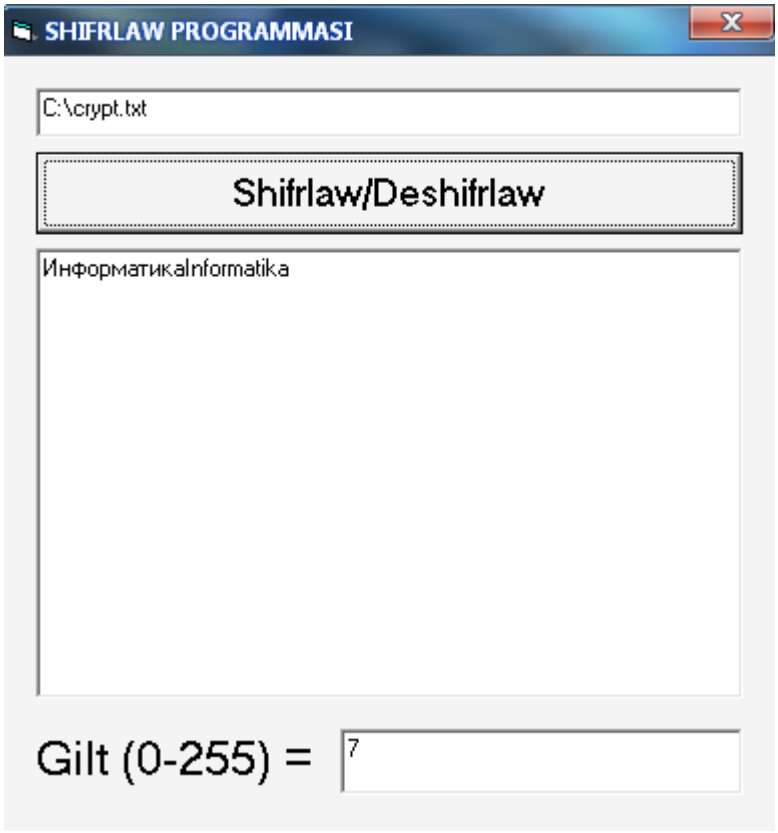
Fayl mazmuni’ ekrang’a shi’g’ari’ladi’

Gilt beremiz. Wol 0 den 255 san arali’g’i’nda boli’wi’ kerek. Biz gilt=7 dep berdik.

Yendi shifrlaw komandasi’n basami’z.

Shifrlaw tabi’sli’ a’melge asi’ri’ldi’.

Yendi bul tekstti qaytadan tikleymiz. Woni’n’ ushi’n Deshifrlaw komandasi’n beremiz.



Deshifrlaw da tabi’sli’ a’melge asi’ri’ldi’.

PROGRAMMA LISTINGI

```
============Modules/Protect(Protect.bas)========


Option Explicit


Public Function codinng1(ByVal CodFile As String) As
String
Dim bolDone As Boolean: bolDone = False
Dim varData  As Byte
Dim byteTempArray As Byte
Dim intFile As Integer
Dim dblIncreas As Long
Dim dblIncrease As Integer
Dim intFile1 As Integer
Dim Num1 As Integer
intFile = FreeFile()
dblIncrease = 0
Num1 = Form1.Text2.Text
Open CodFile For Binary As #intFile
    intFile1 = FreeFile()
    Open CodFile For Binary As #intFile1
        dblIncreas = LOF(intFile)
        DoEvents
        Do While Not bolDone
            Get #intFile, , byteTempArray
                varData = byteTempArray Xor Num1
```

```
            Put #intFile1, , varData
            dblIncrease = dblIncrease + 1
            DoEvents
            If dblIncrease >= dblIncreas Then
                bolDone = True
            End If
        Loop
    Close #intFile1
Close #intFile
End Function
=====================================================
=================Forms/Form1(Form1.frm)===============
Private Sub Load()
Text1.Text = Form2.Text1.Text
Dim intFile, StrPerem, StrTemp
intFile = FreeFile()

Open Text1.Text For Input As #intFile
Do While Not (EOF(intFile))
Input #intFile, StrTemp
StrPerem = StrPerem & StrTemp
Loop
Close #intFile
Text3.Text = StrPerem
End Sub
```

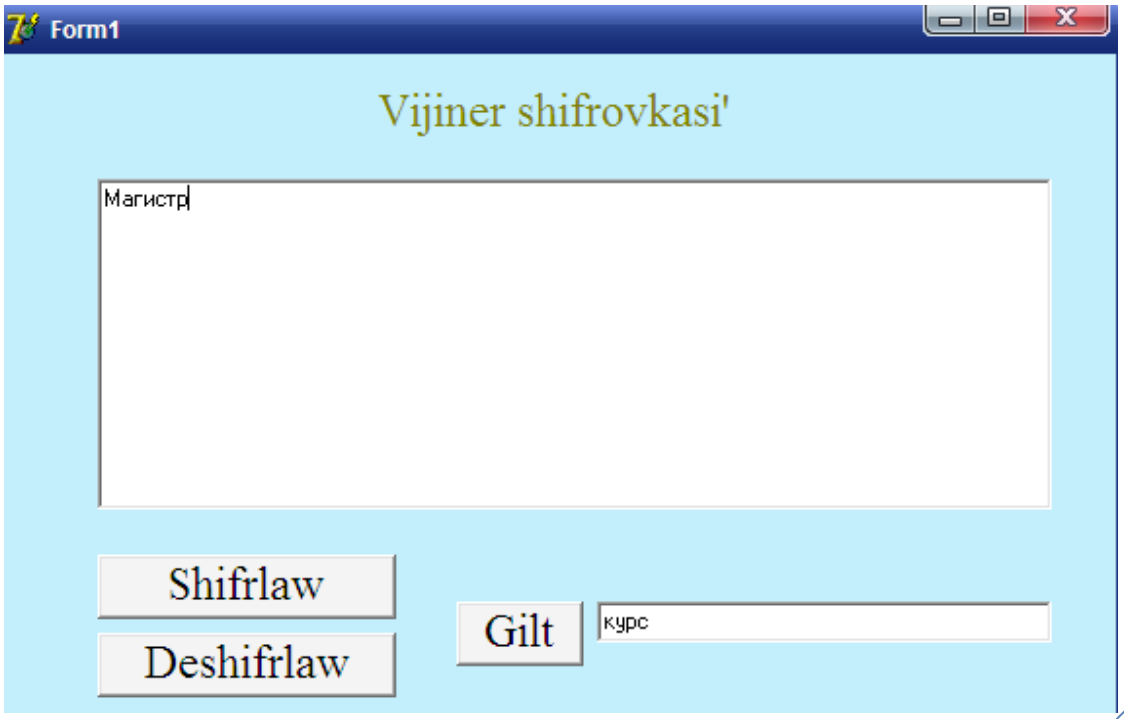
```
Private Sub Command1_Click()
Call codinng1(Text1.Text)
Call Load
Command1.Enabled = True
Command2.Enabled = True
End Sub

Private Sub Command2_Click()
Call codinng1(Text1.Text)
Call Load
Command2.Enabled = True
Command1.Enabled = True

End Sub

Private Sub Form_Load()
Call Load
Command2.Visible = False
Command2.Enabled = False
End Sub
==========================================================
==============Forms/Form2(Form2.frm)================

Private Sub Command1_Click()
Form1.Enabled = True
Form2.Visible = False
```

```
Form1.Visible = True
End Sub

Private Sub Form_Load()

End Sub
```

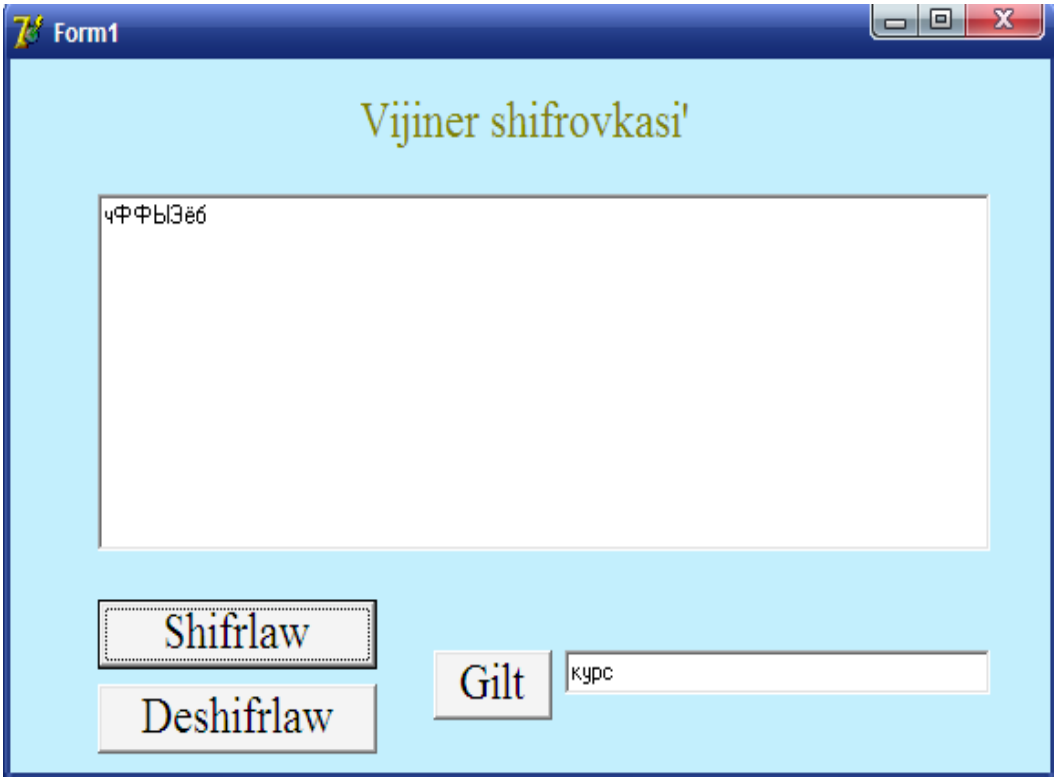
3. Vijiner kestesi ja’rdeminde shifrlaw

Bul formada shifrlanatug’i’n tekst ha’m de gilt boli’p xi’zmet yetetug’i’n so’z soraladi’. Keyin «Shifrlaw» komandasi’ beriledi. Teskti qayta tiklew ushi’n «Deshifrlaw» komandasi’ basi’ladi’.

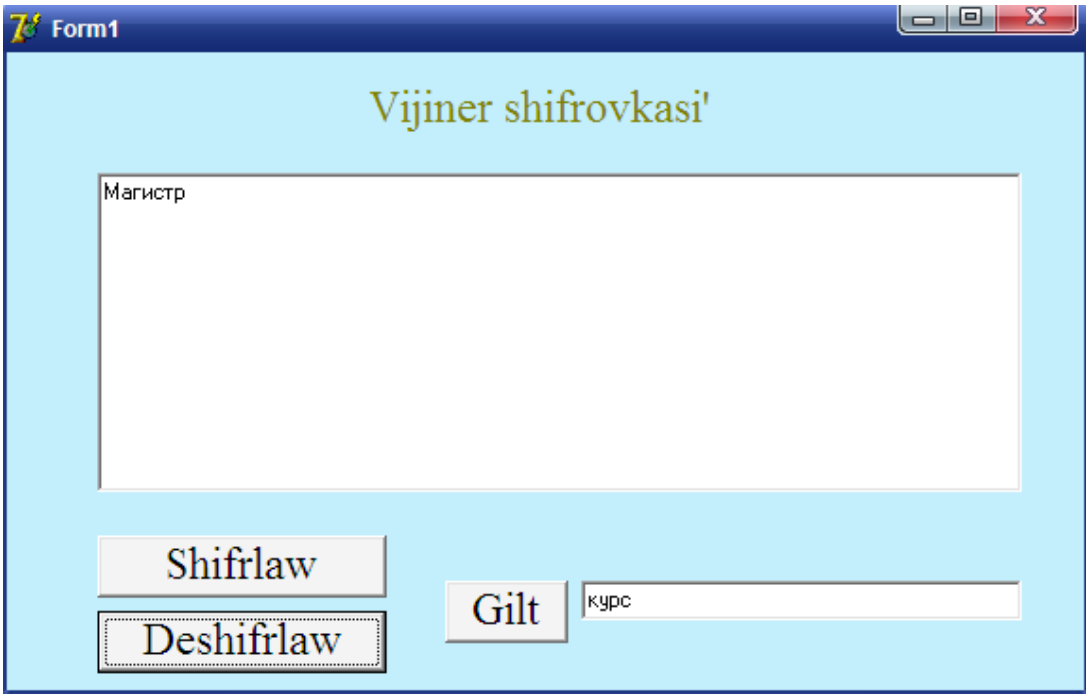
Misali’. «Magistr» so’zin shifrlaw ushin ekrandag’ bos aynag’a jazami’z. Bul so’zdi shifrlaw ushi’n bizge gilt so’zi kerek boladi’. Gilt so’zi «kurs» bolsin.



Shifrlang’an jag’dayi’



Buni’ da’slepki halg’a qaytariw ushin Deshifrlaw knopkasi’n basami’z.



PROGRAMMA LISTINGI

```
procedure TForm1.Button1Click(Sender: TObject);
Var
  s,key, ssh:string;
  i,k,m,l:integer;
const alf='АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ
абвгдеёжзийклмнопрстуфхцчшщъыьэюя';
begin
    s:=Memo1.Text;
  key:='';
  ssh:='';
  while length(key)<length(s) do
key:=key+Edit1.Text;
  for i:=1 to length(s) do
  begin
  k:=pos(s[i],alf)-1;
  m:=pos(key[i],alf)-1;
  if k+m>67 then l:=k+m-67+1 else l:=k+m+1;
  ssh:=ssh+alf[l];
  end;
  Memo1.Text:=ssh;
end;
```

```
    procedure TForm1.Button2Click(Sender: TObject);
    Var
      s,key, dsh:string;
      i,k,m,l:integer;
    const alf='АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ
абвгдеёжзийклмнопрстуфхцчшщъыьэюя';
    begin
        s:=Memo1.Text;
      key:='';
      dsh:='';
      while length(key)<length(s) do
key:=key+Edit1.Text;
      for i:=1 to length(s) do
      begin
      l:=pos(s[i],alf)-1;
      k:=pos(key[i],alf)-1;
      if l-k<0 then m:=l-k+67+1 else m:=l-k+1;
      dsh:=dsh+alf[m];
      end;
      Memo1.Text:=dsh;
    end;
    end;
```

III BAP BOYINSHA JUWMAQ

U’shinsi bapta informaciya qa’wipsizligin ta’miyinlewdin’ kriptografiyali’q metodlari’, kriptografiya tu’sinigi ha’m woni’n’ rawajlani’w tariyxi’, kriptografiya tariyxi’n sha’rtli tu’rde basqi’shqa bo’liniwi, 1) a’piwayi’ kriptografiya 2) formal kriptografiya 3) ilimiy kriptografiya 4) kompyuterli kriptografiya, kriptografiyali’q metodlar ha’m wolardan paydalani’w metodikasi’, zamanago’y kriptografiya informaciya qa’wipsizliginin’ konfidencialli’q, pu’tinlik, autentifikaciya ha’m ta’replerdin’ avtorli’qti’ inkar yete almasli’qlari’ mashqalalari’n ha’l yetiwshi bilim tarawi’, qarsi’las ta’repten baqlawda bolg’an baylani’s kanali’ arqali’ uzati’li’p atri’rg’an xabardi’n’ konfidencialli’g’i’n ta’miyinlew mashqalasi’ aytiladi.

Ja’nede informaciyani’ jasi’ri’wdi’n` tiykarg`i’ kriptografiyali’q metodlari’ni’n` klassifikaciyasi’, basqada kriptografiyali’q metodlar steganografiya, basqa tu`rleri, kesiw-jayi’w, ma`nisi boyi’nsha, mexanikali’q, qi’si’w-ken`eytiw ha’mde kriptograf ha`m kriptoanalitiktin` wazi’ypalari’ haqqinda aytilg`an.

Budan basqada Informaciyani’ kriptografiyali’q qorg’aw ma’selesin programmalasti’ri’w arqali’ sheshiwdi u’yretiw jollari haqqi’nda so’z yetiledi.

JUWMAQLAW

Informaciyali’q ja’miyet jag’dayi’nda informaciya ushi’n gu`res, yen` son`g`i’ xabarlardi’ birinshi boli’p qolg`a kiritiw ha`m wo`zinin` maqsetlerinde paydalani’w, tabi’sqa yerisiw ha`reketleri ku`sheyip barati’r. Ko`pshilik ka`rxanalar wo`zinin` ma`plerin ha`m qarji’lari’n qorg`aw maqsetinde kelgen informaciyani’ filtrlawshi’ ha`r qi’yli’ marshrutizatorlardan, brandmauzerlerden ha`m ruxsatsi’z sistemag`a kiriw jag`daylari’n ani’qlawshi’ programmalar menen qurallang`an bolg`anli’g`i’na qaramastan, bul sharalardi’n` barli’g`i’ biykar boli’wi’ mu`mkin.

Kompyuterlerdi global tarmaqqa biriktiriw barli’q paydalani’wshi’larg’a du’nya ju’zlik torda saqlani’p turg’an mag’li’wmatlar bazasi’na kiriw ha’m qa’legen informaciyani’ ali’w mu’mkinshiligin ashi’p berdi. Soni’n’menen birge, tarmaq kompyuterlerinde saqlani’p turg’an ha’m tarmaq boyi’nsha tarqati’latug’i’n informaciyani’ ha’m ha’r bir adamni’n’ jeke aqi’l miynetin qorg’aw mashqalasi’ payda boladi’. Demek, informaciyani’ ji’ynaw, saqlaw, qayta islew ha’m jetkerip beriw processinde woni’ qorg’aw ju’da’ u’lken mashqala boli’p tabi’ladi’.

Informaciyali’q sistemalar i’qti’yari’y tarawdag`i’ wazi’ypani’ sheshiw maqsetinde za`rur bolgan informaciyani’ ji’ynaw, saqlaw, qayta islew, qi’di’ri’w ha’m ali’sqa uzati’w jumi’slari’n ta`miynleydi. Wolar mashqalalardi’ analiz qi’li’wg`a ha’m jan`a wo`nim jarati’wg`a ja`rdem beredi.

Komp`yuter tarmag`i’ baylani’s kanallari’ ja`rdeminde mag`li’wmatlardi’ tarmaqlangan qayta islewdin` jalg`i’z sistemasi’na jalg`ang`an komp`yuterler ha’m terminallar toplami’ boli’p, wol ko`p mashinali’ birlespenin` yen` joqari’ formasi’ yesaplanadi’. Internet arqali’ pu`tkil dun`ya boylap jayi’li’p ketken neshe ju`z million komp`yuterlerdi ha`r biri ushi’n uli’wma bolg`an informaciyali’q wortali’qqa biriktiriw imkaniyati’ tuwi’ldi’.

Paydalani’wshi’ ko`z qarasi’nan global tarmaq birinshi na`wbette tarmak abonentlerine wo`z-ara mag`li’wmatlar almasi’w, virtual tu`rde baylani’s jasaw imkaniyati’n jarati’p beriwshi "informaciyali’q magistral" wazi’ypasi’n atqaradi’, yekinshiden, wonda bar bolg`an mag`li’umatlar bazasi’

toplami’ dun`ya bilimler bazasi’n quraydi’. Soni’n` menen birge internet bugungi ku`nde dun`ya bazari’n u`yreniwde, marketing jumi’slari’n sho`lkemlestiriwde zamanago`y biznestin` yen` a`hmiyetli qurallari’nan birine aylani’p qaldi’.

Informaciyani’ qorg`awdi’n` da`stu`riy usi’llari’ bolg`an tarmaqlar ara ekranlar yaki marshrutizatorlardag`i’ filtrlew mexanizmleri tek g`ana hu’jimnin` yekinshi - a`melge asi’ri’li’w- basqi’shi’nda iske tu`siriledi. Biraq, qansha qi’mbat bahali’ ha`m ku`shli qorg`aw qurallari’na iye bolsaqta, baslani’p ketken hu’jimdi ha`mme waqi’t toqtati’w mu`mkin bola bermeydi. Wodan da qorg`aw quri’lmalari’n bastan, hu’jim qi’li’wdi’n` birinshi basqi’shi’nan baslaw, yag`ni’y sistemami’z tuwrali’ informaciya ji’ynawg`a jol qoymaw, hu’jimnin` aldi’n ali’w mu`mkinshiligin beredi. Bul hu’jimdi toli’g`i’ menen toqtatpasa da, jaman nietli shaxsti’n` jumi’si’n qi’yi’nlasti’radi’.

Yesaplaw mashinalari’ ha’m elektron baylani’s qurallari’ insan iskerliginin’ barli’q tarawlari’na kirdi. Zamanago’y kriptografiya da wolarsi’z a’mel qi’la almaydi’. Tekstlerdi shifrlaw ha’m deshifrlawdi’ EEM ja’rdeminde pu’tin sanlardi’ qayta islew procesi dep ko’z aldi’mi’zg’a keltirsek boladi’. Al bul operaciyalardi’n’ wori’nlani’w jollari’n pu’tin sanlar ko’pliginde ani’qlang’an belgili bir funkciyalar dep ali’wg’a boladi’. Bulardi’n’ barli’g’i’ kriptografiyada sanlar teoriyasi’ni’n’ metodlari’ payda boli’wi’na ali’p keledi. Wonnan ti’sqari’, bir qatar zamanago’y kriptosistemalardi’n’ turaqli’li’g’i’ tek ayri’m teoriyali’q-sanli’q ma’selelerdin’ quramali’li’g’i’ menen belgilenedi.

O’zbekistan Respublikasi’ Konstituciyasi’nda ha’m Ji’nayat Kodeksinde de kriptografiya jaqi’nda rawajlani’p baslag’ani’na qaramastan, bul tarawda bir qansha jumi’slar islendi. Joqari’ woqi’w wori’nlari’nda kriptografiya boyi’nsha magistratura qa’nigelikleri ashi’ldi, ilimiy izleniwshilerdin’ kandidatli’q ha’m doktorli’q dissertaciya temalari’ tasti’yi’qlandi’. Mashqalani’n’ aktualli’gi’n ha’m a’hmiyetin, bul tarawdi’ rawajlandi’ri’wg’a qarati’lg’an is-ilajlardi’ yesapqa ali’p, tez arada wo’zimizdin’ milliy kriptografiyali’q algoritmler islep shig’i’li’wi’na isenim bildiriwge boladi’.

PAYDALANI’LG`AN A`DEBIYATLAR

1. O’zbekiston Respublikasi Oliy Majlisining Axborotnomasi. – T., 2003. №1. – 2-m.
2. O’zbekiston Respublikasi qonun hujjatlari to’plami. – T., 2011. – №45-46. – 472-m.
3. O‘zbekiston Respublikasining 1993-yil 7-maydagi 848-XII-sonli «Davlat sirlarini saqlash to‘g‘risida»gi qonuni.
4. «O’zbekiston Respublikasida axborotni kriptografik muxofazalash chora-tadbirlari to’g`risida»gi 614-son qarori, 3 aprel 2007.
5. Aloqa va axborotlashtirish sohasida axborot xavfsizligi: Atamalar va ta`riflar. Tarmoq standarti: Ct 45-010:2010.
6. Andronchik A.N., Bogdanov V.V. i dr. Zashita informacii v komp`yuterni’x setyax. – M.-2003.
7. Aripov M., Pudovchenko Yu. Osnovi’ kriptografii. –T.: UzMU-2004.
8. Erosh I.L. Sistema peredachi danni’x s zakri’ti’mi klyuchami // Informatsionni’e sistemi’ v ekonomike i promi’shlennosti /SPb., 1999.
9. Ivanov M.A.. Kriptograficheskie metodi’ zashiti’ informatsii v komp`yuterni’x sistemax i setyax. – M:-.Kudits-obraz. -2001.
10. Moldovyan A.A., Moldovyan N.A., Sovetov B.Ya. Kriptografiya. – SPb.: Izdatel`stvo “Lan`”, 2001.
11. Shnayer B.. Prikladnaya kriptografiya. – SPb.,-2002.
12. Tureniyazova A.I., Niyazimbetova Z. Informaciyani’ qorg’awdi’n’ kriptografiyali’q usi’llari’. Ilim ha’m ja’miyet.,№4 2013
13. Tureniyazova A.I.,Qunnazarov A. Uzliksiz talim sifat va samaradorligini oshirish masalalari. Ilimiy konferentsiya materiallari. Samarqand 2013. 21-22 b.
14. Qunnazarov A. Informatsiya qa`wipsizligin ta`miynlew sistemalari’ni’n` effektivligin asi’ri’w jollari’. Jas ilimpazlardi’n` ilimiy maqalalari’ toplami’. No`kis 2014. 9-10 b.

15. www.microsoft.com/security. Microsoft korporatsiyasi’ni’n` qa`wipsizlik ma`selelerine bag`i’shlang`an sayti’.
16. www.microsoft.com/security/security_bulletins/alerts2.asp. Microsoft ti’n` qa`wpsizlik byulletenine jazi’li’w.
17. www.uzcert.uz
18. www.infocom.uz