WO’ZBEKSTAN RESPUBLİKASI’ BAYLANI’S, İNFORMATİZACİYALASTI’RI’W HA’M TELEKOMMUNİKACİYALI’Q TEXNOLOGİYALAR MA’MLEKETLİK KOMİTETİ

TASHKENT İNFORMACİYALI’Q TEXNOLOGİYALAR UNİVERSİTETİ NO’KİS FİLİALI’

KOMPYUTER İNJİNİRİNGİ FAKULTETİ

«INFORMATIKA HA’M INFORMACION TEXNOLOGIYALAR» KAFEDRASI’

«Karxana servis » bagdari’ni’n’

4-kurs studenti Dosi’mbetov Shamshetdinnin’

PİTKERİW QA’NİGELİK JUMI’SI’

Temasi: ***“Assimetriyali’q kriptosistemalardi’ du’ziwdin’ matematikali’q tiykarlari’“***

Ilimiy basshi’ : _____ f.-m.i.k. A.D.Arziev

Kafedra basli’gi’: _____ t.i.k. Arzi’mbetov T.Z.

NO’KIS- 2014 j.

M A Z M U N I’

KIRISIW ……. 3

§1 Ma’selenin’ qoyi’li’wi’……... 5

§2 Si’rli’ parametrlerdi ani’qlaw ……..…….. 13

§3 *A, u* ha’m *t* lardi’ tabi’w ma’selesi..... 16

§4 Ryukzak ma’selesine tiykarlang’an kriptosistema tu’rleri …….. 24

§5 Ti’g’i’z ryukzaklar…… 38

JUWMAQLAW …….. 48

A’DEBİYATLAR ……..... 50

QOSI’MSHA ……... 51

KIRISIW

Ashi’q giltli kriptosistema koncepciyasi’ Uitfild Diffi ha’m Martin Xellman ta’repinen alg’a su’rildi. Ralf Merkl de bul ma’sele menen wolardan g’a’rezsiz tu’rde shug’i’llandi’. Wolardi’n’ kriptografiyag’a qosqan u’lesi bul –jup giltlerden yag’ni’y shifrlawshi’-deshifrlawshi’ giltlerdi paydalani’w boli’p tabi’ldi’. Bul ideyani’ birinshi ma’rte 1976-ji’li’ Milliy kompyuter konferenciyada (National Computer Conference) Diffi ha’m Xellman ma’sele yetip qoydi’. Bir neshe aylardan son’ wolardi’n’ «Kriptografiyada jan’a bag’dar» (New Derections in Criptography) atamasi’ndag’i’ miyneti jari’q ko’rdi.

Da’slepki jarati’lg’an ashi’q giltli kriptosistemalardi’n’ ko’pshligi talap yetilgen qa’wpsizlikti jetkilikli da’rejede ta’miynley almadi’, al qa’wpsiz degen sistemalar a’meliy jaqtan qollani’w mu’mkin bolmadi’ yamasa wolarda ju’da’ u’lken gilt qollandi’ yamasa shifrlang’annan son’ ali’ng’an kriptotekstin’ wo’lshemi da’slepki kiriwshi tekstin’ wo’lsheminen bir qansha arti’p ketti. Qa’wipsiz ha’m a’meliy jaqtan qollani’w mu’mkin bolg’an algoritmler sani’ ko’p yemes. A’dette bul algoritmler matematikada bar bolg’an qi’yi’n ma’selelerdin’ birine tiykarlanadi’. wolardi’n’ bazi’ birewleri tek giltlerdi bo’listiriw, bazi’ birewleri bolsa shifrlaw, al qalg’anlari’ bolsa tek elektron imza ushi’n jaramli’ boli’p yesaplanadi’.

Biz pitkeriw qa’nigelik jumi’si’nda Ralf Merkl ha’m Martin Xellman ta’repinen jari’ti’lg’an birinshi assimetriyali’ shifrlaw algoritmi bolg’an ryukzak algoritmin qarasti’rami’z. Da’slepki waqi’tta bul algoritm tek mag’li’wmatlardi’ shifrlaw ushi’n qollani’li’wi’ mu’mkin yedi, biraq keyin ala Adi SHamir bul sistemani’ elektron imza ushi’n da qollani’w mu’mkin yekenligin ko’rsetti.

Yen’ da’slepki ashi’q giltli kriptosistemalar tiykari’nda ryukzak haqqi’nda ma’sele jatadi’. wol baslang’i’sh mag’li’wmatlardi’n’ uli’wma ji’ynag’i’ ushi’n qi’yi’n ma’sele boli’p yesaplang’an. Bul ma’sele NP-toli’q ma’seleler klasi’na jatadi’, biraqta bul ma’selege tiykarlang’an kriptosistema turaqli’ yemes yekenligin ko’rsetiw de mu’mkin.

Tiykarg’i’ ideya - ryukzak haqqi’ndag’i’ ma’selenin’ yeki parametrin saylap ali’wdan turadi’, yag’ni’y: ashi’q parametrler ma’seleni qi’yi’nlasti’radi’, al si’rli’ bolsa woni’ an’sat sheshiletug’i’n yetedi. Bunnan basqa bazi’ bir qosi’msha funkciya bar boli’p, woni’n’ ja’rdeminde qi’yi’n ma’sele an’sat ma’selege ali’p keliniledi.

Sistemani’ bunday usi’l menen qarasti’ri’w woni’ RSA kriptosistemasi’n uqsas yekenligin ko’rsetedi yag’ni’y: quramali’ modul boyi’nsha berilgen sannan *e* da’rejeli koren shi’g’ari’w ju’da’ qi’yi’n, biraq yegerde modul a’piwayi’ san bolsa, wonda wol an’sat sheshiledi. Qosi’msha informaciyag’a iye boli’w, atap aytqanda, kriptosistemani’n’ modulin a’piwayi’ ko’beytiwshilerge jiklew, bunday quramali’ ma’seleni bir qansha an’sat ma’selege ali’p keliwge imkaniyat jarati’p beredi. Biraqta RSA ma’selesi menen ryukzak haqqi’ndag’i’ ma’sele arasi’nda ayramshi’li’q bar. Uli’wma aytqanda, ryukzak haqqi’ndag’i’ ma’sele sanlardi’ faktorizaciyalawdi’n’ uli’wma ma’selesinen de quramali’ ma’sele boli’p yesaplanadi’.

Ryukzak haqqi’ndag’i’ ma’sleni sheshiw ju’da’ qi’yi’n bolg’ani’ menen bazi’ bir jag’daylarda bul ma’sele tez sheshimge iye bolatug’i’n baslang’i’sh mag’li’wmatlar klassi’ bar boladi’ ha’m wondag’i’ parametrler progressiv wo’siwshi dep atalatug’i’n izbe-izliklerge tiyisli boladi’. Bul pitkeriw qa’nigelik jumi’si’nda bunday izbe-izliktin’ bir neshe tu’rlerin qarasti’rami’z. Bul ma’selege tiykarlang’an ayi’ri’m kriptosistemalarg’a toqtap wo’temiz. wolardag’i’ si’rli’ parmetrlerdi ani’qlaw ha’m ti’g’i’z ryukzaklarda qollani’latug’i’n izbe-izlikler tu’rin qarasti’rami’z. Tiykari’nan usi’ parametr tu’rlerin qollani’p ryukzak haqqi’ndag’i’ ma’selege tiykarlang’an sistemalardi’ qarap wo’temiz.

§1 Ma’selenin’ qoyi’li’wi’

Kriptografiyada bir ta’repleme funkciya tu’sinigi ken’ qollani’ladi’. Wol berilgen x argumenti ushi’n f(x) funkciyasi’n an’sat yesaplaw, al kerisinshe *f(x)* tan *x* ti’ tabi’w qi’yi’n bolatug’i’n funkciyani’ an’latadi’. Bunday tu’rdegi bir ta’rpleme funkciyalari’ kriptografiyali’q funkciyalar dep ataymi’z.

Meyli bizge ha’r qi’yli’ n won’ pu’tin sanlar turatug’i’n $(a_1, a_2, ..., a_n) = A$ ji’yi’ni’ ha’m ja’ne bir pu’tin won’ α sani’ berilsin. Wonda ryukzak haqqi’ndag’i’ ma’sele: qosi’ndi’si’ α ten’ bolatug’i’n sonday da bir a_i lardi’ tabi’w boli’p tabi’ladi’. A’dette α ryukzak wo’lshemin, al a_i sanlari’ni’n’ ha’r biri ryukzakqa sali’natug’i’n predmetlerdi an’latadi’. Bizge bul jerde ryukzak toli’g’i’ menen tolti’ri’lwi’ mu’mkin bolatug’i’n predmetler ji’yi’ni’n tabi’w ma’selesi qoyi’ladi’.

Ryukzakti’ jaylasti’ri’wdi’n’ an’sat ma’selelerinin’ u’les klasslari’ bar boli’p, wolarda qollani’latug’i’n *A* -tez wo’siwshi *n* ji’yi’nlardan turadi’.

Yegerde ji’yi’ndag’i’ ha’r bir kelesi san da’slepki sanlardi’n’ qosi’ndi’si’nan u’lken ya g’ni’y $j = 2,3,...n$ ushi’n

$$a_j > \sum_{i=1}^{j-1} a_i$$

bolsa, wonda $A = (a_1, a_2, ..., a_n)$ ji’yi’ni’ tez wo’siwshi dep atali’di’.

Da’slep biz berilgen ryukzak wo’lshemi α ushi’n $\alpha \geq a_n$ sha’rtin tekseremiz. Yegerde wori’nlansa, wonda a_n izlenip ati’rg’an qosi’ndi’g’a kirmeydi, keri jag’dayda wol qosi’ndi’g’a kiriwi kerek. Yegerde ji’yi’n tez wo’siwshi bolatug’i’n bolsa, berilgen α ushi’n ryukzak haqqi’ndag’i’ ma’sele jalg’i’z bir sheshimge iye boladi’. Kriptosistemani’ qa’wpsizligin ta’miynlew maqsetinde *A* ji’yi’ni’na moduli ko’beytiw ja’rdeminde qosi’msha a’meller islep na’tiyjede tez wo’siwshi bolmaytug’i’n *B* vektori’na iye bolami’z. Woni’n’ ushi’n

$m > \sum a_i$ alami'z ha'm woni'n' menen wo'z-ara a'piwayi' bolatug'i'n t sani'n ani'qlaymi'z. Bul t g'a keri element m moduli boyi'nsha an'sat tabi'ladi'. Son'i'nan $ta_i (\mathrm{mod}\, m)$ a'melin wori'nlap B ji'yi'ni'ni'n' elementlerin alami'z. Ali'ng'an ji'yi'n mag'li'wmatlardi' shifrlaw ushi'n ashi'q gilt wazi'ypasi'n atqaradi', al t, t^{-1} ha'm m si'r saqlanadi'. Bul ayti'lg'anlar algoritmnin' qi'sqasha wori'nlani'w etaplari' yedi. Yendi biz ryukzak haqqi'ndag'i' ma'selege ken'irek tu'sinik berip wo'temiz.

Ha'r qi'yli' a_i natural sanlardi'n' n $(n \geq 3)$ ta'rtiplesken ji'yi'ni'nan turatug'i'n $A = (a_1, a_2, .., a_n)$ ryukzak vektori' berilsin. Ryukzak haqqi'ndag'i' ma'selede kiriwshi mag'li'wmat (A, α) jupli'g'i' boladi', bunda A-ryukzak vektori', al $\alpha -$ natural san. Yegerde A ni'n' bazi' bir u'les ko'pliginin' elementlerinin' qosi'ndi'si' α g'a ten' bolsa, wonda woni' (A, α) jupli'g'i'ni'n' sheshimi dep aytami'z. Ryukzak haqqi'ndag'i' ma'seleni ayri'm waqi'tlari' wo'lshemler qosi'ndi'si' ha'qqi'ndag'i' ma'sele dep te ataydi'.

Ryukzak haqqi'ndag'i' ma'selede (A, α) jupli'g'i' sheshimge iye yamasa iye yemesligin tabi'w qaraladi'.

A vektori' n yekilik simvollardan turi'wshi' C blokti' shifrlaw ushi'n qollani'ladi'. C dag'i' birler poziciyasi'na sa'ykes keliwshi A ni'n' elementlerin qosi'wdan ibarat boladi'. yegerde bul qosi'ndi'ni' α arqali' belgilesek, wonda deshifrlaw α boyi'nsha C tabi'wg'a yamasa assimetriyali' kriptosistemalardan paydalansaq, wonda α boyi'nsha A ni' tabi'w menen ten' ku'shli boladi'.

Mi'sali' $n = 6$ ha'm $A = (3, 41, 5, 1, 21, 10)$ bolsi'n. Wonda yekilik bloklar (110010) ha'm (101101) ler sa'ykes 65 ha'm 19 si'pati'nda shifrlanadi'. Berilgen A vektori' ushi'n barli'q kriptotekstler 81 den kishi sanlar. $A = (14, 28, 56, 82, 90, 132, 197, 284, 341, 455)$ jag'dayda $\alpha = 55$ teksti sa'ykes u'sh shi'g'i'wshi' tekstke ten' boladi': (1,1,0,0,1,0,0,1,0), (0,1,1,0,1,0,0,0,1,0), (1,0,0,1,1,1,1,0,0,0). Bul jerde A won'nan solg'a qaray woqi'ladi'. Mi'sali' 455 sheshim yemes, sebebi 60=515-455 qosi'ndi'si' tu'rinde

jaza almaymi'z h.t.b. Usi'lay yete woti'ri'p $\alpha = 516$ kriptoteksti de sa'ykes shi'g'i'wshi' tekstke iye yemes. Bul jag'dayda A ni'n' to'rt izbe-iz sani'ni'n' birewi de qosi'ndi'g'a kirmeydi, al qalg'an sanlardi'n' qosi'ndi'si' ju'da' kishi yekenligin ko'remez. $\alpha = 517$ushi'n jalg'i'z sa'ykes keletug'i'n shi'g'i'wshi' tekst (1,1,1,0,1,1,1,0,0,0). Bunday tu'rdegi mi'sallardi' qarasti'rg'anda: bazi' bir kiriwshi mag'li'wmatlarda ryukzak ma'selesin sheshiw kriptoanaliz ushi'n an'sat yemes yekenligin ko'remiz.

Deshifrlaw ma'selesi bir ma'nisli boli'wi' ushi'n A vektori' α g'a uqsas qa'siyetke iye, yag'ni'y barli'q (A,α) lar tek bir sheshimge iye boli'wi' kerek. Bunday tu'rdegi ryukzak vetorlari'n *inektiv* vetorlar dep ataymi'z.

Bazi' bir A vektori' ushi'n (A,α) lar an'sat sheshiledi. Bunday na'tiyjege yerisiw ushi'n vektor tez (progressiv) wo'siwshi qasiyetke iye boli'wi' kerek. Bunday izbe-izlik Merkl-Xellman kriptosistemasi'nda qollani'ladi'.

Yegerde ha'm tek sonda g'ana barli'q j=2,3,..,*n* ushi'n

$$a_j > a_{j-1} \text{ (sa'ykes } a_j > \sum_{i=1}^{j-1} a_i \text{)}$$

ten'sizligi wori'nlansa, wonda $A = (a_1, a_2, .., a_n)$ vektori' tez wo'siwshi dep ataladi'. A vektori' ushi'n

$$\max A = \max(a_j | 1 \le j \le n)$$

ani'qlaymi'z.

Meyli x teris yemes san bolsi'n. [x] arqali' x ti'n pu'tin bo'legin, yag'ni'y yen' u'lken pu'tin $\le x$.

$\forall x$ ha'm $m \geq 2$ ushi'n, x ti' m ge bo'legende qalatug'i'n yen' kishi teris yemes qaldi'qti' $(x, \mathrm{mod}\, m)$ dep belgileyik.

$$(x, \mathrm{mod}\, m) = x - [x/m] \cdot m$$

yekenligin an'sat tekseriwge boladi'.

Yendi moduli ko'beytiw tu'siniginin' yeki variantan qarasti'rami'z. Pu'tin $m > \max A$ ha'm natural $t < m$ ler ushi'n yen' u'lken uli'wma bo'liwshi $(t, m) = 1$ bolatug'i'n A vektori' berilsin. Yegerde $B = (b_1, ...b_n)$ vektori' komponentleri

$$b_i = (ta_i, \mathrm{mod}\, m),\ i = 1, ..., n$$

ali'natug'i'n bolsa, wonda B vektori' m moduli ha'm t ko'beytiwshisine yamasa qi'sqasha *(t,m)* jubi'na qarata moduli kobeytiw ja'rdeminde A dan ali'ng'an dep aytami'z. $(t, m) = 1$ sha'rti

$$tu \equiv 1 (\mathrm{mod}\, m)$$

ha'm $1 \leq u < m$ bolatug'i'n keri $t^{-1} = u$ sanni'n' bar yekenligine kepillik beredi. Bul bizge A vektori' m ha'm u g'a qarata B dan modulli ko'betiw ja'rdeminde ali'natug'i'ni'n an'latadi'.

Yegerde $m > \max A$ sha'rti qatan' sha'rt, yag'ni'y $m > \sum_{i=1}^{n} a_i$ menen almasti'ri'lsa, wonda B vektori' A dan m ha'm t g'a qarata qatan' moduli ko'beytiwden alai'nadi'. Biz bul jerde keri jag'day wori'nlanadi' dep ayta almaymi'z, sebebi $m > \sum_{i=1}^{n} b_i$ ten'sizligi barli'q waqi'tta da wori'nlana bermeydi. Biraqta, a'lbette A vektori' B dan m ha'm u qarata moduli ko'beytiwden ali'nadi'.

Kriptosistemani' du'ziwshi A,t,m,B saylaydi', bul jerde A vektori' tez wo'siwshi, al B vektori' A dan m ha'm t boyi'nsha qatan' moduli ko'beytiwden ali'nadi' ha'm wol shifrlaw wazi'ypasi'n atqaradi'. N uzi'nli'qtag'i' yekilik bloklardi' B vektori' ja'rdeminde shifrlag'annan son' ali'ng'an β sani' adresatqa jiberiledi. Mag'li'wmatqa ni'zamsi'z iyelik yetken ta'rep (B,β) jupli'g'i' ushi'n ryukzak ma'selesin sheshiwi kerek boladi'. Sistemani' jarati'wshi' bolsa, $\alpha = (u\beta, \mathrm{mod}\, m)$ yesaplaydi' ha'm (A,α) jupli'g'i' ushi'n ryukzak ma'selesin an'sat sheshedi. Bul qalayi'nsha a'melge asi'ri'latug'i'ni'n to'mendegishe lemma ko'rsetedi.

Lemma 1. *Meyli* $A = (a_1, a_2, .., a_n)$ *tez wo'siwshi vektor ha'm* B *vektori'* A *dan* m *ha'm* t *boyi'nsha qatan' moduli ko'beytiwden ali'ng'an ha'm* $u = t^{-1} (\mathrm{mod}\, m)$, $\beta -$ *qa'legen natural san ha'm* $\alpha = (u\beta, \mathrm{mod}\, m)$ *bolsi'n. Wonda to'mendegishe tasti'yi'qlawlar wori'nli' boladi':*

(I) (A,α) *ryukzak ma'selesi ha'mme waqi'tta sheshemge iye ha'm yegerde sheshim bar bolsa, wonda wol jalg'i'z boladi'.*

(II) (B,β) *ryukzak ma'selesi jalg'i'z bir shesheimge iye.*

(III) yegerde (B,β) *ushi'n sheshim bar bolsa, wonda wol* (A,α) *ni'n' jalg'i'z sheshimi menen u'stpe-u'st tu'sedi.*

Da'liylleniwi.

(I). Biz joqari'dag'i' mi'salda tez wo'siwshi vektordi' qollang'anda ryukzak ma'selesi belgili bir waqi'tta A vektori'n won'nan solg'a qarata bir ma'rte woqi'w arqali' sheshiletug'i'ni'n ko'rsettik. Bul ma'sele yen' arti'g'i' menen bir sheshimge iye boladi'.

(II) ha'm (III). Meyli n uzi'nli'qqa iye D vektori' (B,β) ma'selesinin' sheshimi, yag'ni'y $BD=\beta$ bolsi'n. Bunnan:

$$\alpha = u\beta = uBD = u(tA) = AD(\mathrm{mod}\, m)$$

m sani' A vektori'ni'n' komponentlerinin' qosi'ndi'si'nan asi'p ketpeytug'i'n bolg'anli'qtan, $AD<m$ ja'nede $\alpha<m$ sha'rtinen ani'qlama boyi'nsha $\alpha=AD$ boladi'. Bunnan D vektori' (A,α) ma'selenin' jalg'i'z sheshimi menen u'stpe-u'st tu'sedi. Bul jerde (I'I'I') da'liylledik ha'm biz (B,β) ma'selesinin' qa'legen sheshimin qarasti'ri'p wol (A,α) ma'selesinin' jalg'i'z sheshimi menen u'stpe-u'st tu'setug'i'nli'g'i'n ko'rsettiw joli' menen (I'I') ni de da'liyllegen bolami'z.

Mi'sal 1. Meyli n=10 ha'm tez wo'siwshi vektor

$$A=(103,107,211,430,863,1718,3449,6907,13807,27610)$$

Moduldi m=55207 dep alayi'q. YU'UB(t,m)=1 bolatug'i'nday yetip t=25236 alami'z ha'm keri element m moduli boyi'nsha $t^{-1}=u=1061$ ten'. Haqi'yqattan da 1061*25236-1=485*55207 Na'tiyjede qatan' modul ko'beytiwden to'mendegishe vektordi' alami'z

B=(4579,50316,24924,30908,27110,17953,32732,16553,22075,53620)

Mi'sali'

25236*103=4579+47*55207 ha'm 1061*4579=103+88*55207,

25236*1718=17953+785*55207 ha'm 1061*17953=1718+345*55207,

25236*27610=53620+12620*55207 ha'm 1061*53620=27610+1030*55207.

Bul jerde B vektori' ashi'q, al A,t,u,m si'rli' giltti quraydi'. A'lbette m ha'm t yamasa u lardi' bile woti'ri'p basqa shamalardi' da yesaplaw mu'mkin. Yendi biz

INFINLAND so’zin *B* vektori’n qollani’p shifrlayi’q. Da’slep tan’bali’ kodlaw ushi’n *A-Z* deyingi ha’riplerdi 1-26 shekmgi, al probeldi 0 sani’ menen belgileymiz. Tan’bali’ kodlardi’ yekilik sanaq sistemasi’ ja’rdeminde an’latami’z.

Ha’rip	San	Ekilik sanaq sistemasi’nda jazi’li’wi’
PROBEL	0	00000
A	1	00001
B	2	00010
C	3	00011
D	4	00100
E	5	00101
F	6	00110
G	7	00111
H	8	01000
I	9	01001
J	10	01010
K	11	01011
L	12	01100
M	13	01101
N	14	01110
O	15	01111
P	16	10000
Q	17	10001
R	18	10010
S	19	10011
T	20	10100
U	21	10101
V	22	10110
W	23	10111
X	24	11000
Y	25	11001
Z	26	11010

Shifrlawda berilgen *B* vektori’n qollang’ani’mi’zda yekilik blokti’n’ uzi’nli’g’i’ 10 bolg’anli’qtan teksti yeki ha’ripten turi’wshi’ bloklarg’a aji’ratqan maqul. To’mendegi tablicada berilgen tekstin’ bloki, wog’an sa’ykes keletug’i’n yekilik kodi’ ha’m shifrlang’an blokti’n’ wonli’q sanaq sistemasi’ndag’i’ jazi’li’wi’ keltirilgen.

IN	01001	01110	14786
_F	00000	00110	38628
IN	01001	01110	14876
LA	01100	00001	128860
ND	01110	00100	122701

Birinshi 148786 sani'n deshifrlaymi'z. Da'slep $1061 \cdot 148786 = 2859 \cdot 55207 + 25133$ yekenligin ani'qlaymi'z ha'm (*A*,25133) ryukzak ma'selesin qarasti'rami'z. Sheshim *A* vektori'n won'nan solg'a qarap woqi'wdan ali'nadi'. Yegerde shep bag'anadag'i' san *A* ni'n' qarasti'ri'li'p ati'rg'an komponentinen kishi bolsa, wonda 1 di jazami'z ha'm bag'anadag'i' jan'a san komponentadan kelesi sandi' ali'p taslawdan ali'nadi'. Keri jag'dayda 0 simvoli' jazi'ladi' ha'm sheptegi san wo'zgermeydi. Bul a'mellerdin' na'tiyjesinde to'mendegilerge iye bolami'z:

San	**A komponetasi'**	**Simvol**
25133	27610	0
25133	13807	1
11326	6907	1
4419	3449	1
970	1718	0
970	836	1
107	430	0
107	211	0
107	107	1
0	103	0

IN blok ali'natug'i'n yekilik vektor - won' bag'anani' to'mennen joqari' qaray woqi'wdan kelip shi'g'adi'. Yekinshi san 38628 di deshifrlawda da'slep 20714 alami'z ha'm woni'n' menen de joqari'dag'i' a'mellerdi wori'nlaymi'z.

Eskertiw. Meyli biz keri ta'rtipte ha'reket yeteyik. Mi'sali' bizin' tekstimizde *OR* bloki bir neshe ma'rte ushi'rassa, wonda woni' *A* vektori' menen shifrlay woti'ri'p 7665 ti alami'z. Biraq (*B*,7665) jupli'g'i' sheshimge iye yemes. A'piwayi' yetip aytqanda, biz a'dettegi sanlardi'n' ten'ligin, wolardi'n' modul boyi'nsha ten'liginen keltirip shi'g'ara almaymi'z, sebebi *m* sani' *B* vektori'ni'n' komponentlerinin' qosi'ndi'si'nan kishi. Haqi'yqattan da

$$7665 \equiv 173286 \ (mod\ 55207)$$

Sonli'qtan biz 173286 sani' menen a'meller islewimiz kerek.

§2 Si'rli' parametrlerdi ani'qlaw

Meyli bizge $B = (b_1, ...b_n)$ ryukzak vektori' belgili bolsi'n ha'm woni' shifrlashwi' gilt si'pati'nda qarasti'rayi'q. Ja'nede *B* vektori' tez wo'siwshi *A* vektori'ni'n' komponentlerin *t* g'a ko'beytip *m* moduli menen sali'sti'rg'annan ali'natug'i'nli'g'i' belgili. Bizge *A* vektori', *m* ha'm *t* sanlari' belgisiz boli'p wolardi' wolardi' tabi'w ma'selesi qoyi'lsi'n. Bizdi yen' qi'zi'qti'ratug'i'ni', bul *m* ha'm $t^{-1} = u(\mathrm{mod}\, m)$ sanlari' boli'p tabi'ladi'. Bul yeki *m* ha'm *u* sanlardi' bile woti'ri'p *A* vektori'n an'sat yesaplawi'mi'z mu'mkin ha'm qa'legen kriptoteksti deshifrlaw imkaniyati'na iye bolami'z. *t* boyi'nsha *u* di' yesaplaw yamasa kerisinshe *u* boyi'nsha *t* ni' yesaplaw Evklid algoritmin qollani'p tez a'melge asi'ri'w mu'mkin.

Bizge bul jerde «tek shifrlawshi' gilt belgili» degen sha'rt qoyi'ladi'.

Bul paragrafta A. Shamirdin' kriptoanalitikali'q usi'li' qarasti'ri'ladi'. Biz woni'n' na'tiyjesinde polinomial algoritmge iye bolalami'z

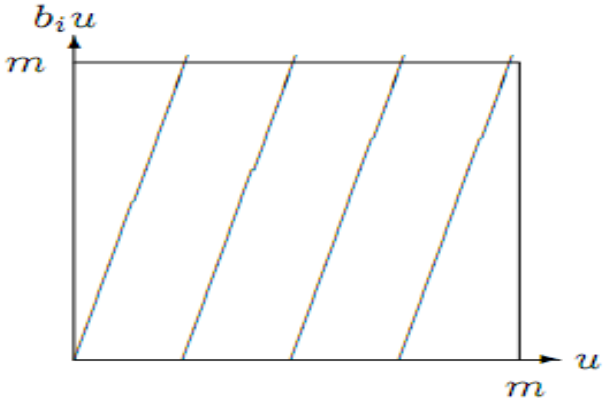
Polinomial algoritm haqqi'nda ayta woti'ri'p kiriwshi *B* vektori'ni'n' wo'lshemin ani'qlawda itibarli' boli'w kerek. Sebebi algoritmnin' polinomialli'g'i' sol vektordi'n' wo'lshemine baylani'sli' boladi'. Biz wo'lshemi sheksiz wo'siwshi *B* ryukzak vektorlar klassi'n qarasti'ri'wi'mi'z kerek. *B* vektordi'n' wo'lshemi degende yeki parametr: komponentler sani' n ha'm b_i individual komponentlerinin' wo'lshemin tu'sinemiz. Yegerde bul parametrlerdin' qa'legenin joqari'dan shegaralasaq, wonda kelip shi'g'atug'i'n ryukzak haqqi'ndag'i' ma'sele polinomial waqi'tta sheshiliwi mu'mkin.

Haqi'yqattan da, yegerde ha'r bir qarali'p ati'rg'an vektorda qa'legen b_i ler bazi' bir *S* turaqli'si'nan asi'p ketpese, wonda usi'nday pu'tin sanli' vektorlardi'n' sani' shekli ha'm sondayda bir fikserlengen shegara bar boli'p, wonda qa'legen qarasti'ri'li'p ati'rg'an ryukzak haqqi'ndag'i' ma'sele 2^C koefficenti menen si'zi'qli' waqi'tta sheshiliwi mu'mkin.

A'dette wo'lshem si'pati'nda komponentler sani' n ali'nadi' ha'm wog'an baylani'sli' komponentler ushi'n shegara ani'qlanadi'. Bunday tu'rdegi komponentler ushi'n shegara matematikali'q ko'z qarastan jasalma boli'p yesaplanadi' ha'm uli'wma ma'seleni shegaralaydi'.

Algoritmdi du'ziwde u keri ko'beytiwshisin ha'm kriptosistemani' jarati'wshi' haqi'yqattan qollang'an m modulin izlew sha'rt yemes. Bizdi *B* vektori'n moduli ko'beytiwden payda bolg'an *A* vektori' tez wo'siwshi bolatug'i'n u ko'beytiwshisi ha'm *A* ni'n' komponentlerinin' qosi'ndi'si'nan u'lken bolatug'i'n m moduli, yag'ni'y bul sha'rtler wori'nlanatug'i'n qa'legen (u,m) jubi' qanaatlandi'radi'. Bul (u,m) di' si'rli' jupli'q dep ataymi'z. yegerde biz jupli'qti'n' birewin tapsaq, wonda lemma 1 tiykari'nda ali'ng'an tez wo'siwshi vektordi' paydalani'p deshifrlawdi' baslawi'mi'z mu'mkin.

(u,m) jupli'g'i'n tabi'w ushi'n biz da'slep $b_i u \pmod m$ funkciyasi'ni'n' grafigin $\forall i = 1,...,n$ ushi'n qarasti'rami'z. $b_i u \pmod m$ funkciyasi'ni'n' grafigi tuwri' si'zi'qli' kesindilerden turadi', al $u = pm/b_i$, $p = 1,2,...$ ma'nisi u'zilis tochkalari' boli'p tabi'ladi' (1-su'wret).



1-su'wret

$b_1 u \pmod m = a_1$ da u - wo'zgeriwshi yemes, al izlenip ati'rg'an keri ko'beytiwshi boli'p yesaplanadi'. a_1 - tez wo'siwshi vektordi'n' birinshi komponentasi' ha'm m barli'q komponentalardi'n' qosi'ndi'si'nan arti'q bolsa, wonda a_1 - m ge sali'sti'rg'anda ju'da' kishi boli'wi' kerek. Bunnan u ma'nisi b_1 funkciyasi'ni'n' bazi'-bir minimumi'na jaqi'n boli'wi' kerek yekenligi kelip shi'g'adi'. Kriptosistemani' jarati'wshi' $\forall i$ ushi'n $b_i / a_i < 1$ sha'rti wori'nlani'wi' kerek yekenligin umi'tpaw kerek. Bul jag'dayda bazi' bir arali'qlar ku'tilgennen de u'lken boladi' ha'm wol kriptoanalitik ushi'n ko'p qi'yi'nshi'li'qlar tuwdi'radi'.

Usi'lay dawam yete woti'ri'p u ma'nisi b_2 nin' bazi' bir minimumi'na jaqi'n dep pikir ju'ritemiz. Bul b_1 ha'm b_2 funkciyalari'ni'n' qandayda bir minimumlari' bir-birine jaqi'n boli'w kerek degen juwmaqqa ali'p keledi.

Bul processti dawam yete woti'ri'p grafikte basqada iymek si'zi'qlardi' ko'rip shi'g'ami'z ha'm n sani'n tabi'wdi'n' worni'na biz iymek si'zi'qlardi'n' minimumlari'ni'n' «ji'ynali'w tochkasi'»n tabi'wg'a ha'reket yetemiz. Bul ha'r bir ali'ng'an iymekliklerdin' minimumlari'nan turatug'i'n bazi' bir kishi intervaldi' du'ziw menen ten' ku'shli boladi'. Du'zilgen intervalda u ma'nisin tabami'z.

§3. *A, u* ha'm *t* lardi' tabi'w ma'selesi

Bul pargrafta tez wo'siwshi vektordi', moduldi ha'm ko'beytiwshini tabi'w ma'selesin qarasti'rami'z. Biz bul jerde ryukzak vektori'ni'n' komponentlerin shamasi'n n ge qarata sheklemeymiz. Yegerde B vektori'ni'n' komponentalar sani' bazi' bir k sani' menen sheklengen bolsa, wonda bul soraw an'sat boli'p yesaplanbaydi'. Haqi'yqattanda, wolar ushi'n 2^k saylap ali'w varianti' jetkilikli yemes. Uli'wma aytqanda bul sorawg'a juwap tabi'lsa, wonda sa'ykes ryukzak ma'selesi an'sat sheshiledi.

Ani'qlama. *Tek ha'm tek sonda g'ana, yegerde A vektori' tez wo'siwshi vektori' bar boli'p, A dan qatan' modulli ko'beytiwden B vektori' ali'nsa, wonda B ryukzak vektori' superjetiskenli vektor dep ataladi'. Yegerde* A_0 *tez wo'swshi vektor bolatug'i'nday* $A_0, A_1, ...A_r = B$ *tu'rindegi vektorlar izbe-izligi tabi'li'p ha'm* $\forall i = 0,1,.....r-1$ *ushi'n* A_{i+1} *vektori'* A_i *den qatan' moduli ko'beytiwden ali'nsa, wonda* $r \le 1$ *ushi'n B vektori'* $r-$*giperjetiskenli dep ataladi'.*

Teorema 1. *Qa'legen* $r-$*giperjetiskenli vektor inektiv boladi'. Sonli'qtan qa'legen superjetiskenli vektor da inektiv boli'p yesaplanadi'.*

Da'liylleniwi. Teorema to'mendegishe yeki (I) ha'm (II) faktti'n' saldari' boli'p tabi'ladi'.

(I) qa'legen tez wo'siwshi vektor inektiv boli'p tabi'ladi'.

Haqi'yqattan da, joqari'da qarasti'rg'an A tez wo'siwshi vektor bolg'anda (A,α) ryukzak ma'selesi yen' arti'g'i' menen tek bir sheshimge iye.

(II) Qatan' moduli ko'beytiw wo'zinin' inektivliligin saqlaydi'.

Meyli B vektori' A dan (m,t) jubi'na qarata qatan' moduli ko'betiwden ali'ng'an ha'm bazi' bir C ha'm C' ekilik vektorlari' ushi'n $BC = BC'$ bolsi'n. Bize A vektori' B dan (m,u) moduli ko'beytiwden ali'natug'i'ni' belgili, bunda $u = t^{-1}$. Uyg'ari'wi'mi'z boyi'nsha $uBC = uBC'$ boladi', wonda $AC \equiv AC' \pmod m$. m sani' A vektori'ni'n' komponentlerinin' qosi'ndi'si'nan arti'q bolg'anli'qtan, m moduli boyi'nsha son'g'i' sali'sti'ri'w a'piwayi' ten'lik penen jazi'li'wi' kerek, yag'ni'y $AC = AC'$. (I) den $\tilde{N} = \tilde{N}'$, sonli'qtan B vektori' inektiv boli'p tabi'ladi'.

Lemma 2. *Yegerde A vektori' wo'siwshi yamasa tez wo'siwshi bolsa, wonda wo'siwshi izbe-izliktegi ha'r bir vektor (A,t,m) u'shligi tiykari'nda sa'ykes tu'rde wo'siwshi yamasa tez wo'siwshi vektor boladi'.*

Da'liylleniwi. $a_{i-1} < a_i$ ten'sizligi $[ta_{i-1}/m] \le [ta_i/m]$ qatnasi'n keltirip shi'g'aradi'. Yegerde A wo'siwshi vektor bolsa, wonda ha'r bir $A(k)$ vektori' da wo'siwshi boladi'.

Meyli

$$\sum_{j=1}^{i-1} a_j < a_i$$

bolsi'n. Bunnan

$$\sum_{j=1}^{i-1}[ta_j/m] \le [\frac{(t\sum_{j=1}^{i-1}a_j)}{m}] \le [ta_i/m]$$

kelip shi'g'adi'. A tez wo'siwshi vektor bolsa, wonda $A(k)$ da tez wo'siwshi yekenligin an'latadi'.

Lemma 3. *Yegerde* $B=(b_1,...,b_n)$ *vektori' A dan* (m,t) *qarata modulli (qatan' modulli) ko'beytiwden ali'nsa, wonda B vektori' da ha'r bir* $A(k)$ *ni'* $(m+kt,t)$ *qarata modulli (qatan' modulli) ko'beytiwden ali'nadi'.*

Da'liylleniwi. Sha'rt boyi'nsha $b_i=(ta_i, \mathrm{mod}\, m),\ 1\le i\le n$

$(t,m+kt)=1$ yekenligi belgili. Qa'legen k ushi'n

$$t(a_i+k\cdot[ta_i/m]) = b_i+[ta_i/m]\cdot m+[ta_i/m]\cdot kt = \\ = b_i+[ta_i/m](m+kt)$$

al $b_i < m+kt$ bolg'anli'qtan

$$(t(a_i+k\cdot[ta_i/m]), \mathrm{mod}(m+kt)) = b_i$$

alami'z. Bul B vektori' $A(k)$ dan $(m+kt,\ t)$ qarata moduli ko'beytiwden ali'natug'i'ni'n an'latadi'.

Meyli B vektori' A dan (m,t) qarata qatan' ko'beytiwden ali'ng'an bolsi'n. Bul

$$\sum_{i=1}^{n} a_i < m$$

bunnan

$$\sum_{i=1}^{n}(a_i + k[ta_i / m]) < m + \sum_{i=1}^{n} k[ta_i / m] \le$$
$$\le m + k[t(a_1 + ... + a_n) / m] \le m + k \cdot [t] = m + kt$$

kelip shi'g'adi'.

Yendi (*A,t,m*) u'shligin qarasti'rayi'q, bunda $A = (a_1,...,a_n)$ ryukzak vektori', $m > \max A, t < m$ ha'm $(t,m) = 1$. (A_1, t_1, m_1) u'shligin (A,t,m) u'shliginin' transponirlengen tu'ri dep ataymi'z, bunda

$$m_1 = t, \quad t_1 = (-m, \bmod t),$$
$$A_1 = ([ta_1 / m],...,[ta_n / m]),$$

Lemma 4 *Meyli* (A_1, t_1, m_1) - (A,t,m) *ni'n' transponirlengen tu'ri bolsi'n. Yegerde B vektori' A dan (m,t) qarata qatan' moduli ko'beytiwden ali'ng'an ha'm* $\max B < t$ *bolsa, wonda B vektori'* A_1 *den* (m_1, t_1) *qarata (qatan') moduli ko'beytiwden ali'ng'an ha'm* $\max B < t$ *bolsa, wonda B vektori' da* A_1 *den* (m_1,t_1) *qarata (qatan') moduli ko'beytiwden ali'nadi'. Yegerde B-tez wo'siwshi vektor bolsa, wonda wol* $t' \ge \max B$ *menen* (A', t', m') *tez wo'siwshi boli'p tabi'ladi'.*

Da'liylleniwi. $t_1 < t$ yekenligi belgili. U'shlikti woni'n' transponirlengen tu'ri menen almasti'ri'w procedurasi'n ta'kirarlay woti'ri'p $t' \le \max B$ bolatug'i'nday u'shlikti alami'z.

Haqi'yqattan da, meyli V vektori' (m, t) qarata moduli ko'beytiwden ali'ng'an ha'm $t > \max B$ bolsi'n. $1 \le i \le n$ ushi'n $(ta_i, \bmod m) = b_i$ alami'z. Bul

$$t[ta_i / m] \equiv b_i - ta_i \equiv b_i$$

yekenligin an'latadi'. Sebebi $b_i \le \max B < t$ bolg'anli'qtan biz bul ten'likti

$$(t_1[ta_i / m], \mod t) = b_i$$

dep jazi'wi'mi'z mu'mkin. Bul *B* vektori' *A* dan (m_1, t_1) qarata moduli ko'beytiwden ali'natug'i'ni'n ko'rsetedi. Bul qatan' moduli ko'beytiw ushi'n da wori'nli' boladi', sebebi, yegerde

$$m > \sum_{i=1}^{n} a_i$$

bolsa, wonda

$$t > \sum_{i=1}^{n} ta_i / m \le \sum_{i=1}^{n} [ta_i / m$$

Lemmai'n' keyingi tasti'yi'qlawi'n da'liyllewde bizge A vektori' tez wo'siwshi yekenliginen A_1 vektori' da tez wo'siwshi bolatug'i'ni'n ko'rsetiw jetkilikli. A tez wo'siwshi vektor yekenligi $2 \le i \le n$ ushi'n

$$\sum_{j=1}^{i-1} ta_j / m < ta_i / m$$

bolatug'i'ni'ni' an'latadi'. Bunnan

$$\sum_{j=1}^{i-1} [ta_j / m] \le [ta_i / m] \qquad (*)$$

Bul jerde ten'lik belgsi wori'nli' dep alsaq, wonda

$$\sum_{j=1}^{i-1} m[ta_j / m] = m[ta_i / m]$$

bunnan

$$\sum_{j=1}^{i-1} (ta_j - b_j) = ta_i - b_i$$

kelip shi'g'adi'. woni'

$$b_i - \sum_{j=1}^{i-1} b_j = t(a_i - \sum_{j=1}^{i-1} a_j)$$

tu'rinde jazi'wg'a da boladi'. Bul jerde *t* koefficenti won' bolg'anli'qtan

$$t \le b_i - \sum_{j=1}^{i-1} b_j < b_i \le \max B$$

alami'z. Bul $t > \max B$ sha'rtine qarama-qarmi' bolg'anli'qtan biz (*) da qatan' ten'sizlik belgisi boli'wi' kerek yekenligin ko'remiz. Bizde *i'*- qa'legen, sonli'qtan A_1 vektori' tez wo'siwshi boli'p tabi'ladi'.

Endi izbe-izlik kemiwshi bolg'an jag'daydi' qarasti'rami'z.

Lemma 5. *Meyli B vektori' A dan (m,t) qarata moduli ko'beytiwden ali'ng'an ja'nede* $m > 2\max B$ *ha'm* $t \le \max B$ *bolsi'n. wonda B vektori' da A(-1) den (m-t,t) qarata moduli ko'beytiwden ali'nadi'. Bunnan basqa, yegerde A wo'siwshi vektor bolsa, wonda A(-1) de tez wo'siwshi boladi'.*

Da'liylleniwi. $A = A(0) = (a_1,...,a_n)$ ha'm $B = (b_1,...,b_n)$ belgileymiz. wonda $A(-1),\ 1 \le i \le n$ vektori'ni'n' i'-shi' komponentasi' $a_i - [ta_i / m]$ boladi'. Woni' t-g'a ko'beyte woti'ri'p

$$ta_i - t[ta_i / m] = b_i + m[ta_i / m] - t[ta_i / m]$$
$$= b_i + (m-t)[ta_i / m] \equiv b_i \pmod{(m-t)}$$

alami'z. Bizde $m - t > \max B \ge b_i$ bolg'anli'qtan

$$(t(a_i - [ta_i / m]) \bmod (m-t)) = b_i$$

iye bolami'z.

$$m > 2t \quad \text{dan} \quad m - t > t \qquad (*)$$

ha'm $(t, m-t) = 1$ boladi'. Keri tasti'yi'qlaw isleymiz: bazi' bir i' ler ushi'n $a_i - [ta_i / m] \ge m - t$. Buni' t g'a ko'beyte, tA_i, an'latpasi'n ha'm $m > 2$ qollana woti'ri'p

$$t(m-t) \le b_i + (m-t)[ta_i / m] < \frac{m}{2} + (m-t)[ta_i / m]$$

alami'z. Bunnan

$$\frac{m}{2} > (m-t)(t - [ta_i / m])$$

bul jerde $t > [ta_i / m]$ bolg'ani' ushi'n wol (*) qarsi' keledi. Lemmani'n' yekinshi tasti'yi'qlawi'n da'liyllew ushi'n $A(-1) = (e_1,....,e_n)$ belgilewin kiritemiz. Meyli i' qa'legen ha'm $1 \le i \le n-1$. A(-0) tez wo'siwshi bolg'anli'qtan bazi' bir $\alpha \ge 1$ ushi'n

$$a_{i+1} = a_i + \alpha$$

boladi'. Da'slep $\alpha > 1$ bolsi'n, wonda

$$\begin{aligned} e_{i+1} &= a_i + \alpha - [t(a_i + \alpha)/m] \\ &\geq a_i + \alpha - (1 + [ta_i/m] + [t\alpha/m]) \\ &= e_i + (\alpha - 1) - [t\alpha/m] > e_i \ . \end{aligned}$$

bul jerde birinshi ten'sizlik $[x+y] \leq [x] + [y] + 1$ bolg'ani' ushi'n, al yekinshi bolsa (*) boyi'nsha

$$[t\alpha/m] \leq t\alpha/m < \frac{\alpha}{2}$$

bolg'anli'g'i' sebepli wori'nli' boladi'.

Meyli $\alpha = 1$ bolsi'n. Bul jag'ayda $[t\alpha/m] = 0$. Yegerde

$$[t(a_i + 1)/m] = [ta_i/m]$$

Bolsa, wonda biz $e_{i+1} > e_i$ iye bolami'z. Sonli'qtan

$$[t(a_i + 1)/m] = [ta_i/m] + 1 \qquad (**)$$

dep uyqarami'z. (**) sha'rti $e_{i+1} = e_i$ an'lati'wi' mu'mkin. (**) won' ta'repin $\beta + 1$ dep belgileymiz. Sonda

$$m\beta \leq ta_i < m(\beta + 1) \leq t(a_i + 1)$$

$ta_i < m(\beta + \frac{1}{2})$ dep ali'p (*) boyi'nsha

$$ta_i + 1 < m(\beta + \frac{1}{2}) + t = m(\beta + 1) + t - m/2 < m(\beta + 1)$$

degen qarama-qarsi'li'qqa iye bolami'z. Sonli'qtan $ta_i \geq m(\beta + \frac{1}{2})$. Biraqta $b_i = ta_i - \beta m \geq m/2$ bolg'anli'qtan $m \leq 2b \leq 2 \max B$ boladi' ha'm (**) wori'nlanbaydi'.

Mi'sali'. $A = (1,14,23,66,105), \quad t = 87, \quad m = 374$

Onda $B = (87,96,131,132,159)$ boladi' ha'm $t \leq \max B$, $m > 2 \max B$. $A(-1) = (1,11,18,51,81)$ Bul tez wo'siwshi vektor bolmaydi'.

Lemma 6. *Lemma 5 tasti'yi'qlawi'n qanaatlandi'ratug'i'n* A, B, m *ha'm t ja'nede* $(A(-1), t, m-t)$ *wo'siwshi izbe-izligin qarasti'rayi'q. Meyli* $(C, t, m), C = (c_1, ..., c_n)$ *usi' izbe-izliktin' birinshi u'shligi bolsi'n. Wonda* $C = A$ *boladi'.*

Da'liylleniwi. Lemma 5 uqsas $A(-1) = (e_1, ..., e_n)$ bolsi'n. Qa'legen $i, \ 1 \leq i \leq n$ ushi'n a_i, c_i, e_i komponentalari'n a'piwayi' a, c, e tu'rinde belgileymiz. Kemiwshi ha'm wo'siwshi izbe-izliktin' ani'qlamasi' boyi'nsha $c = e + [te/(m-t)]$ ha'm $e = a - [ta/m]$ boladi'. $a = c$ ten' yekenligin da'liyllew ushi'n

$$[te/(m-t)] = [ta/m] \qquad (*)$$

yekenligin ko'rsetiw jetkilikli. 3 ha'm 5 lemmalardan

$$ta \equiv tc \pmod{m} \text{ yamasa } a \equiv c (\mathrm{mod}\, m)$$

bunnan

$$[te/(m-t)] \equiv [ta/m] \bmod(m) \qquad (**)$$

qatnasi' kelip shi'g'adi'. Yegerde kvadrat skobkadag'i' an'latpalardi'n' ayi'rmasi'ni'n' absalyut shamasi' m ge yeseli ha'm (*) sha'rti wori'nsi'z bolg'an jag'dayda (**) sha'rti wori'nlani'wi' mu'mkin. Bunday boli'wi' mu'mkin yemes yekenligin ko'rsetemiz, sebebi yeki an'latpada m nen kishi.

Haqi'yqattan da $m-t > \max A(-1) \geq e$, wonda

$$[te/(m-t)] < t < m.$$

boladi'. $t/m = x$ dep ha'm $[y] \leq y$ ten'sizligin qollani'p (**) won' jag'i'n bahalaymi'z.

$$\begin{aligned}
[ta/m] &\leq xa = x(e+[ta/m]) \leq x(e+[ta/m])) \\
&\leq x(e+x(e+x(e+[ta/m]))) \leq e(x+x^2+\ldots+x^p[ta/m]) \\
&\leq e/(1-x)+x^p[ta/m] = me/(m-t)+x^p[ta/m] \\
&< m+x^p[ta/m]
\end{aligned}$$

Bul ten'sizlik qa'legen u'lken p lar ushi'n wori'nlanadi' ha'm wondag'i' $x^p[ta/m]$ qosi'li'wshi'si' qa'legenshe kishi yetip saylap ali'w mu'mkin. Bunnan $[ta/m] < m$ kelip shi'g'adi'.

§4 Ryukzak ma'selesine tiykarlang'an kriptosistema tu'rleri

Bul paragrafta biz kriptoanalitikali'q hu'jimlerge ha'r qi'yli' usi'llarda qarsi' tura alatug'i'ni'n ko'rsetiwshi ryukzak ma'selesine tiykarlang'an kriptosistema tu'rlerin qarasti'rami'z.

Biz $A=(a_1,...,a_n)$ ryukzak vektori' ashi'q ha'm bazi' bir $K=(k_1,...,k_n)$ gilti si'rli' bolg'an jag'daydi' qarasti'rami'z, bunda $k_i=0,1$. Bul gilt shifrlawda ha'm deshifrlawda da qollani'ladi'.

To'mendegishe belgilew kiritemiz:

$\oplus$ belgisi arqali' *mod* 2 boyi'nsha bitli qosi'w a'melin belgileymiz. Bul vektorlar ushi'n da wori'nli' boladi'. Sebebi $1\oplus1=0$ ha'm $(1,1,0,1,0)\oplus(1,1,1,0,0)=(0,0,1,1,0)$.

$$t=[\log_2(1+\sum_{i=1}^{n}a_i])+1$$

dep belgileymiz, bunda a_i din' qa'legen summasi' *t* razryadli' yekilik san si'pati'nda an'lati'ladi' ha'm ha'r bir a_i tek bir ma'rte g'ana kelip shi'g'adi'.

Yesletip wo'tkenimizdey, *A* ashi'q, al yekilik vektor K – jabi'q (si'rli') boladi'. Shifrlani'w kerek bolg'an tekst *t* uzi'nli'qtag'i' $P=(p_1,...,p_t)$ tu'rinde yekilik bloklarg'a aji'rati'ladi'. Ha'r bir *P* ushi'n $R=(r_1,...,r_n)$ yekilik vektori' saylap ali'nadi'. Bunnan son'

$$A(K\oplus R)=\sum_{i=1}^{n}(k_i\oplus r_i)a_i$$

qosi'ndi'si' du'ziledi, bunda $K\oplus R$ vektor-bag'ana si'pati'nda qarasti'ri'ladi'. Meyli *S* usi' qosi'ndi'ni'n' *t* uzi'nli'qtag'i' yekilik su'wretleniwi bolsi'n, yegerde

za’ru’r bolsa *t*-ni’n’ shep ta’repine nollerdi qosi’p jazi’w mu’mkin. *P* shifrlang’an tu’ri to’mendegishe boladi’:

$$C=(L,R),\ \text{bunda}\ L=S\oplus P$$

Usi’ni’n’ menen birge $(n+t)$ - bitli kriptotekst *t* bitli kiriwshi tekstke sa’ykes keledi. Kriptoteksttin’ son’g’i’ *n* biti *K* ni’ beretug’i’n bolsa, wonda *K* ni’ biliwshi shaxs *S* ti an’sat yesaplawi’ mu’mkin.

(P,C) jupli’g’i’n biliwshi kriptoanalitik *S* ti $L\oplus P=S\oplus P\oplus P=S$ ja’rdeminde tez yesaplaydi’. Usi’nday usi’l menen ali’ng’an *S* ani’q bir *P* tekstine sa’ykes keledi *R* belgili bolg’ani’ menen *K* ni’ tabi’w ryukzak ma’selesin sheshiwge ali’p keledi. Al bul ju’da’ quramali’ boli’p yesaplanadi’.

Meyli kriptoanalitikke jetkilikli da’rejede kiriwshi teksttten turi’wshi’ bizi’ bir jupli’q, yag’ni’y tekst ha’m kriptotekst yag’ni’y ani’g’i’raq yetip aytqanda wog’an u’shlik $(P_i,L_i,R_i),\ i=1,\ldots,n$ belgili bolsi’n.

n-bitli *T* ha’m *U* vektorlari’ni’n’ koordinatalari’ni’n’ ko’beymesin $T*U$ dep belgileyik. Yegerde *T* ha’m *U* dag’i’ *i’*-shi komponenta 1 ge ten’ bolsa, wonda $T*U$ degi *i’*-shi komponenta da 1 ge ten’, yag’ni’y

$$T\oplus U=T+U-2(T*U)$$

Haqi’yqattan da *n*=1 ushi’n wori’nli’ boladi’. Ten’lik yeki *n*-bitli vektor ushi’n wori’nli’ dep, indukciya usi’li’ ja’rdeminde *n*+1 – bitli vektor ushi’n da wori’nlanatug’i’ni’n ko’rsetemiz. + ha’m – belgileri a’dettegi qosi’w ha’m ali’wdi’ an’latadi’. Mi’sali’

$$11010\oplus 10111=01101=13=11010+10111-2\cdot 10010=26+23-2\cdot 18$$

bul jerde yekilik vektorlar u’tir ha’m skobkasi’z jazi’lg’an.

Yendi kriptoanalitik $k_{i'}$ ler ushi'n n belgisizli n -si'zi'qli' ten'lemeler sistemasi'na iye boladi'.

$$S_i = A(K + R_i) = A(K + R_i - 2(K * R_i)), \qquad 1 \le i \le n$$

Yegerde bul sistemani'n' ani'qlawshi'si' 0 ge ten' bolsa, wonda K tez tabi'ladi'.

Mi'sali' $A = (2,3,4,5,6,7)$ wonda $n = 6$ ha'm $t = 5$ $K = 110011$. Bul kriptosistemada A ni'n' inektivliligi talap yetilmeydi, sebebi deshifrlaw A komponentlerinin' wo'zin beredi. Wolar summalanadi' ha'm ryukzak haqqi'ndag'i' ma'sele sheshimge iye bolmaydi'.

$P_i = 01010$ tekstin $R_1 = 101010$ ja'rdeminde shifrlaymi'z, yag'ni'y $K \oplus R_1 = 011001$ bunnan $S_1 = 3 + 4 + 7 = 01110$ ha'm $C_1 = 00100101010$. P_1 ha'm C_1 di bile woti'ri'p kriptoanalitik $S_1 = 00100 \oplus 01010 = 01110$ yesaplaydi'. Yendi K ni' ali'w mu'mkin bolg'an $K \oplus R_1$ di tabi'w ushi'n $(A,14)$ ryukzak haqqi'ndag'i' ma'seleni sheshiw kerek, sebebi $K \oplus R_1 \oplus R_1 = K$ $R_1 = K$ boladi'. R_1 vektori' C_1 den ali'nadi'. Sonli'qtan tek (P_1, C_1) jupli'g'i'n biliw

$$C_2 = 1111001010, \quad C_3 = 0111011110, \quad C_4 = 0011101110$$
$$C_5 = 1111000101, \quad C_6 = 0011101101.$$

kriptotekstlerin deshifrlawg'a mu'mkinshilik bermeydi.

Meyli kriptoanalitikke (P_i, C_i) $1 \le i \le 6$ belgili bolsi'n, bunda

$$P_2 = 10011, \ P_3 = 00001, \ P_4 = 10101, \ P_5 = 01110, \ P_6 = 00001$$

Yendi k_i belgisizleri ushi'n si'zi'zi'qli' ten'leieler sistemasi'na iye bolami'z. Meyli i=1 bolsi'n, wonda $S_1 = 14 = AR_1 + A(K - 2(K * R_1))$

Bunnan

$$2 = -2k_1 + 3k_2 - 4k_3 + 5k_4 - 6k_5 + 7k_6$$

ha'm usi'g'an uqsas $S_2 - S_6$ ten'lemelerinen

$$\begin{aligned}
-2 &= 2k_1 - 3k_2 + 4k_3 - 5k_4 + 6k_5 - 7k_6,\\
-6 &= -2k_1 - 3k_2 - 4k_3 - 5k_4 + 6k_5 - 7k_6,\\
0 &= 2k_1 - 3k_2 - 4k_3 - 5k_4 - 6k_5 + 7k_6,\\
6 &= 2k_1 + 3k_2 - 4k_3 + 5k_4 - 6k_5 + 7k_6,\\
-14 &= 2k_1 - 3k_2 - 4k_3 + 5k_4 - 6k_5 - 7k_6.
\end{aligned}$$

alami'z. Bul sistema *k* ni'n' jalg'i'z sheshimin beredi. Haqi'yqattan da 3 ha'm 5 ten'lemede $k_3 = 0$, 2 ha'm 5 den $k_1 = 1$ kelip shi'g'adi'. k_i ler yekilik tu'rdegi wo'zgeriwshiler boli'p tabi'ladi'. k_2, k_4, k_6 ler 0 ge ten'. Son'g'i' ten'lemede k_1 ha'm k_3 ma'nislerin worni'na qoysaq

$$-16 = 3k_2 + 5k_4 - 6k_5 - 7k_6$$

boladi'. Bunnan k_4 nolge ten' bolatug'i'n jalg'i'z wo'zgeriwshi yekenligin ko'rsetedi. Al bul bolsa qalg'an wo'zgriwshilierdin' birge ten' yekenligin an'latadi'.

Yendi ashi'q gilt bazi' bir vektordi' izbe-iz qatan' moduli ko'beytiwden ali'ng'an ryukzak vektori' bolsi'n, bul jerde izbe-izlik tez wo'siwshi boli'wi' sha'rt yemes. Modul ha'm ko'beytiwshi si'rli' «lazeykani'» du'zedi. Bul informaciyag'a iyelik yetiw kriptoteksti deshifrlaw ushi'n jetkilili boli'p yesaplanadi'.

Kriptosistemani' jarati'wshi' qa'legen inektiv $A_1 = (a_1^1, ..., a_n^1)$ ryukzak vektori' qatan' moduli ko'beytiw sha'rtlerin qanaatlandi'ratug'i'n t_1 ko'beytiwshisi ha'm m_1 modulin saylap aladi', yag'ni'y

$$1 \le t_1 < m_1, \ (t_1, m_1) = 1, \ m_1 > \sum_{i=1}^{n} a_i^1$$

$A_2 = (a_1^2, ..., a_n^2)$ vektori' A_1 den (m_1, t_1) qarata qatan' moduli ko'beytiwden ali'ng'an bolsi'n. yendi t_2 ha'm m_2 di qatan' moduli ko'beytiw sha'rti wori'nlanatug'i'nday yetip saylap alayi'q.. Meyli $A_3 = (a_1^3, ..., a_n^3)$ vektori' A_2 den (m_2, t_2) qarat qatan' moduli ko'beytiwden ali'ng'an vektor bolsi'n. Bul process qashan $A_n = (a_1^n, ..., a_n^n)$ - A_{n-1} den (m_{n-1}, t_{n-1}) qarata moduli ko'beytiwden ali'natug'i'n vektor tabi'lg'ang'a shekem dawam yetedi. Kriptosistemani' jarati'wshi' A_n vektori'n shifrlaw ushi'n ashi'q boladi', al $(m_i, t_i), 1 \le i \le n-1$ jubi' si'r saqlanadi'. $(m_i, t_i), 1 \le i \le n-1$ ja'rdeminde $t_i \pmod{m_i}, 1 \le i \le n-1$ ushi'n u_i keri elemnetin an'sat yesaplaw mu'mkin. α_n kriptoteksti ali'ng'annan son'

$$\sum_{i=1}^{n} a_i^n x_i = \alpha_n \qquad (*)$$

bolatug'i'nday n-yekilik $x_1, ..., x_n$ wo'zgeriwshilerin tabi'w kerek $n-1$. moduli ko'beytiwden keyin

$$\alpha_i = (u_i, \alpha_{i+1}, \bmod m_i), \ 1 \le i \le n-1$$

sha’rtin qanaatlandi’ratug’i’n α_i sani’n ani’qlaymi’z. Bul α_i sanlari’ keri ko’beytiwshilerdi qollani’p (*) ni’ izbe-iz moduli ko’beytiwden ali’ng’an boli’p, wol ten’lemenin’ won’ ta’repin quraydi’. Sonda biz

$$\sum_{i=1}^{n} a_i^j x_i = \alpha_j, \quad j = 1,...,n$$

tu’rindegi *n* si’zi’qli’ ten’lemeler sistemasi’na iye bolami’z. Bul sistemadan x_i belgisizlerin tabi’ladi’. Yegerde A_1 vektori’ inektiv bolsa, wonda bir ma’nisli yemeslik saqlani’p qaladi’ ha’m wol sistemani’n’ ha’r bir ten’lemesinde qatnasadi’.

A’piwayi’ mi’sal si’pati’nda to’mendegini qarasti’rami’z.

$$A_1 = (3,2,6), \quad t_1 = 13, \qquad m_1 = 19,$$
$$A_2 = (1,7,2), \quad t_2 = 2, \qquad m_2 = 11,$$
$$A_3 = (2,3,4)$$

$u_2 = 6$ ha’m $u_1 = 3$ boladi’. Bul to’mendegi ten’lemeler sistemasi’na ali’p keledi:

$$\begin{aligned} 2x_1 + 3x_2 + 4x_3 &= 6, \\ x_1 + 7x_2 + 2x_3 &= 3, \\ 3x_1 + 2x_2 + 6x_3 &= 9, \end{aligned}$$

bunnan jalg’i’z yekilik vektor 101 ali’nadi’, biraqta sistema uli’wma sheshimge iye, yag’ni’y $x_2 = 0,\ x_1 = 3 - 2x_3.$

Kelesi qarasti’ratug’i’n ryukzak sistemasi’ elektron imza ushi’n da qollani’w mu’mkin. woni’n’ ushi’n biz ryukzak haqqi’ndag’i’ ma’seleni to’mendegishetu’rlendiremiz, yag’ni’y $n \geq 3$ ushi’n $a_1,...,a_n$ tu’rindegi $n+2$

natural sanlari', α ha'm m - berilgen, bunnan basqa barli'q a_i ler ha'r qi'yli' ha'm $m > \max\{a_i | 1 \le i \le n\}$. Bizden

$$\sum_{i=1}^{n} a_i c_i \equiv \alpha \pmod{m}$$

sali'sti'ri'wi'nda $(c_1,...,c_n)$ sheshimlerin tabi'w talap yetiledi, bunda ha'r bir c_i ler $0 \le c_i \le \lfloor log_2 m \rfloor + 1$ sha'rtin qanaatlandi'radi'. a_i sanlari' qosi'ndi'da bir neshe ma'rte qatnasi'wi' mu'mkin. Biraqta ta'krarlani'w sani' kishi boladi' ha'm wol moduldegi razryadlar sani'nan asi'p ketpeydi.

Bunday tu'rdegi ryukzak sistemasi' qalayi'nsha elektorn imza ushi'n qollani'w mu'mkin yekenligin qarap wo'temiz. Xabardi' imzalawshi' $A=(a_1,...,a_n)$ vektori'n ha'm m sani'n saylap ali'p ryukzak haqqi'ndag'i' qi'yi'n ma'seleni payda yetedi. Bul ma'seleni bazi' bir si'rli' informaciya ja'rdeminde tez ha'm an'sat sheshiwge boladi'. Si'rli' informaciyani' paydalani'p ha'm (*) sheshe woti'ri'p α xabari'n imzalaydi' yag'ni'y: $(c_1,...,c_n)$ ji'yi'ni' α xabari' ushi'n imzani' du'zedi. Bul imzalang'an xabardi' ali'wshi' imzani'n' haqi'yqi'yli'g'i'n (*) g'a qoyi'p tekserip ko'redi. Yegerde adresat yamasa kriptoanalitik bazi' bir α' xabari' ushi'n imzani' qa'lbekilestirmekshi bolsa, wonda wol (A,m,α) u'shligi menen ani'qlang'an ryukzak haqqi'ndag'i' ma'seleni sheshiwi kerek boladi'. Ryukzak sistemasi'n saylap ali'wda qosi'msha: barli'q α xabari' imzag'a iye boli'wi', yag'ni'y (*) qa'legen usi'nday α ler ushi'n sheshimge iye boli'wi' kerek degen talaplar qoyi'ladi'.

Yendi *t*- uzi'nli'qtag'i' yekilik su'wretleniwge iye a'piwayi' *m* sani'n qarasti'rayi'q (a'dette $t = 200$). Meyli $H = (h_{ij})$ wo'lshemi $t \times 2t$ matrica

bolsi'n, woni'n' elementleri $\{0,1\}$ den ali'nadi' ha'm A wo'lshemi $2t$ bolg'an vektor-bag'ana boli'p wol

$$HA \equiv \begin{pmatrix} 2^0 \\ 2^0 \\ \vdots \\ 2^{t-1} \end{pmatrix} \pmod{m}$$

sha'rtin qanaatlandi'radi', bul jerde $2t$ belgisizli t sali'sti'ri'w bar. Biz qatar ha'm bag'analar ushi'n sa'ykes $0 \le i \le t-1$ ha'm $1 \le j \le 2t$ belgilewlerin kiritemiz.

A vektori'ni'n' a_i komponenti tosi'nnanli' san si'pati'nda qaraladi' ha'm 2^0 den 2^{t-1} shekemgi 2 nin' qa'legen da'rejesi, wolardi'n' bazi' birlerinin' m-moduli boyi'nsha qosi'ndi'si' si'pati'nda an'lati'li'wi' mu'mkin.

A vektori' ha'm m- sani' ashi'q boladi', al H bolsa si'r saqlanadi'. α xabari' $[1,...,m-1]$ kesindisindegi sanlar, al woni'n' imzasi' (*) qanaatlandi'ratug'i'n $C = (c_1,...,c_{2t})$ vektori' boladi', bunda $n = 2t.$

Imzani' (*) ja'rdeminde tekserip ko'riwge boladi'. woni' qa'lbekilestiriw joqari'da ko'rsetkenmizdey ju'da' qi'yi'n ma'sele boli'p yesaplanadi'.

Basqa ta'repten qarag'anda imzani' jarati'w si'rli' H ti' paydalana woti'ri'p an'sat a'melge asi'ri'wi'mi'z mu'mkin. woni'n' ushi'n α xabari'n imzalaw ushi'n biz α ni' 2 nin' da'rejelerinin' qosi'ndi'si' si'pati'nda jazami'z

$$\alpha = \sum_{t=0}^{t-1} b_i 2^i$$

b_i-bul α -ni'n' yekilik su'wretleniwinin' won' ta'repindegi *(i'+1)* razryad. Biz

$$c_j = \sum_{i=0}^{t-1} b_i h_{ij},\ 1 \le j \le 2t$$

yetip ali'w mu'mkin dep uyg'arami'z. c_j - (*) da talap yetilgenindey *m*-yekilik su'wretleniwindegi *t* razryadlar sani'nan asi'p ketpeydi. Ja'nede

$$\begin{aligned}\alpha &= \sum_{i=0}^{t-1} b_i 2^i \equiv \sum_{i=0}^{t-1} b_i \sum_{j=1}^{2t} a_j h_{ij} \\ &= \sum_{j=1}^{2t} (\sum_{i=0}^{t-1} b_i h_{ij})\, a_j = \sum_{j=1}^{2t} c_j a_j \pmod m\end{aligned}$$

Imzani' jarati'w ha'm woni' tekseriw ushi'n qosi'msha tek qosi'w a'melin wori'nlaw za'ru'r boladi'.

Ayti'p wo'tilgen sistema xabardi' jasi'ri'w ushi'n arnalg'an yemes, sebebi wolar ashi'q kanallar arqali' jiberiledi. Imzalaw processinin' qa'wpsizligine keletug'i'n bolsaq, wonda wog'an si'zi'qli' algoritmlerge tiykarlang'an hu'jimler jasali'wi' mu'mkin. Haqi'yqattan da jetkilikli da'rejede bir neshe xabar –imza jupli'g'i'na iye bola woti'ri'p *H* matricasi'n yesaplaw mu'mkin.

Qa'wpsizlik ma'selesi α xabari'n imzalawdan aldi'n woni' randomizaciyalaw joli' menen sheshiledi. Bul mi'sali'

$$\alpha' = (\alpha - \sum^{2} t_{j=1} r_j a_j, \mathrm{mod}\, m)$$

bunda $R = (r_1, \ldots, r_{2t})$ tosi'nnanli' yekilik vektor. Son'i'nan α' ler ushi'n C' imzasi' tabi'ladi', keyin $C'+R$ di α ushi'n imza si'pati'nda paydalani'w mu'mkin, sebebi

$$\alpha \equiv \alpha' + RA \equiv C'A + RA = (C'+R)A \pmod m$$

Mi'sal: moduli m=25, yekilik su'wretleniwi 11101. H bolsa 5×10 wo'lshemli tosi'nnanli' matrica bosi'n

$$H=\begin{pmatrix}1\,0\,1\,1\,0\,1\,1\,1\,0\,0\\0\,1\,0\,1\,1\,1\,0\,0\,1\,0\\1\,1\,1\,0\,0\,0\,0\,1\,1\,1\\0\,0\,1\,1\,0\,1\,0\,0\,0\,1\\1\,1\,1\,1\,1\,0\,0\,0\,0\,1\end{pmatrix}$$

dep saylap alami'z. Mi'sal si'pati'nda

$$A=(14,15,19,16,3,24,10,5,2,7,)$$

alami'z ha'm barli'q bes sali'sti'ri'wdi' da wori'nlaymi'z. Mi'sali' u'shinshi sali'sti'ri'w

$$14+15+19+5+2+7=62\equiv4 \pmod{29}$$

tu'rinde boladi'. Yekilik jazi'li'wi' keri ta'rtipte 01101 bolg'an $\alpha=22$ xabari' ushi'n H ti' paydalana woti'ri'p $C=2322210122$ imzasi'n alami'z. Imzani'n' duri'sli'g'i'

$$CA=196\equiv22 \pmod{29}$$

ja'rdeminde tekseriledi. Usi'g'an uqsas kiriwshi 9, 8, 20 ha'm 1 tekstleri ushi'n imzalar sa'ykes 1022021101, 0011010001,2221100112 i 1011011100 boladi'. Kiriwshi teksti ha'riplerdin' sanlar menen kodlang'an tu'ri si'pati'nda qarasti'ri'ladi', yag'ni'y ha'r bir ha'rip beligili bir san menen an'lati'ladi'.

Son'i'nda $\alpha=22$ xabari'ni'n' imzasi'n randomizaciyalaw ma'selesin qarap wo'teyik. woni'n' ushi'n tosi'nnan R=1011010000 saylap,

$\alpha' = (22 - 73, \mathrm{mod}\, 29) = 7$ alami'z. α' ushi'n imza 2222121221 boli'p ha'm bunnan α ushi'n randomizaciyalang'an imza 3233131221 iye bolami'z.

Keyingi qarasti'ratug'i'n kriptosistemami'zda baslang'i'sh *A* vektori' tez wo'siwshi boladi'. Bul *A* vektori'n komponentlerine qosi'msha a'meller qollani'p, wonnan payda bolg'an vektor tez wo'siwshi izbe-izlik yemes tu'rine ali'p kelemiz.

Meyli qarali'p ati'rg'an ryukzak vektori'ni'n' komponentlerin *n* menen ha'm $g = [\log_2 n] + 1$ dep belgileyik ha'm $n < 2^g$. Meyli r_1 ha'm r_2 ler – qa'legen natural sanlar bolsi'n. R_1^i ha'm R_2^i sanlari'n $0 \le R_j^i < 2^{rj}, 1 \le j \le 2, 1 \le i \le n$ sha'rtlerin qanaatlandi'ratug'i'nday yetip saylap alami'z.

$$a_i = R_1^i 2^{n+g+r_2} + 2^{g+r_2+i-1} + R_2^i$$

ani'qlaymi'z. a_i ler ($1 < I' < n$) to'mendegishe tu'rde bolwi' mu'mkin:

Razryadlar nomeri	r_1	n	g	r_2
Razryadlar	R_1^i	0...010...0 *n...i...*1	0...0	R_2^i

R_1^i di belgilew bul- a_i din' tez wo'siwshi yekenligin ha'm R_2^i bloki'n belgilew bul- qatan' moduli ko'beytiw na'tiyjesin jasi'ri'wdan ibarat.

Nollerden turi'wshi' *g* bloki R_2^i sani'n qosi'w ushi'n buferli zona wazi'ypasi'n atqaradi': wol tez wo'siw sha'rtin an'latatug'i'n *n* razryadli' birlik blok ishine ko'shiwlerdin' aldi'n aladi'. Haqi'yqattan da

$$\sum_{i=1}^{n} R_2^i < m2^{r_2} < 2^{g+r_2}$$

Meyli *t* ha'm *m* lar $A = (a_1, ..., a_n)$ ushi'n qatan' moduli ko'beytiw sha'rtin qanaatlandi'rsi'n. Wonda *(t, m)* boyi'nsha *A* vektori'nan qatan' moduli ko'beytiwden ali'ng'an *B*= (*b*,…,b_n) vektori' shifrlaw ushi'n gilt wazi'ypasi'n atqaradi'. t, m, r_1, r_2 sanlari' si'rli' lazeykani' du'zedi. Bul sanlardi' biliw xabardi' tez deshifrlawg'a mu'mkinshilik beredi. Meyli *n* sani' *t* g'a *m* moduli boyi'nsha keri element bolsi'n. β kriptoteksti ushi'n $\alpha = (u\beta, \mathrm{m\ o\ d}\ m)$ belgilew kiritemiz. Wonda β g'a sa'ykes keliwshi tekst α ni'n' yekilik ko'riniste jazi'lg'an *n* razryadli' blok boladi'. Wol keyingi r_2+*g* razryadlardi' si'zi'p taslawdan ha'm *n* razryadi'n keri woqi'wdan ali'nadi'.

Mi'sali' *n*=5, *g*=3. Shifrlawshi vektor

B=(62199, 61327, 13976, 16434, 74879)

Adresatqa $m = 75000,\ n = 22883 (\ t = 1547),\ r_2 = 4$

belgili. Meyli kriptotekst 151054 bolsi'n. 75000 moduli boyi'nsha 22883 ko'beytiwden 43682 sani' ali'nadi'. Bul sanni'n' yekilik jazi'li'wi'

43682 = 1010 1010 1010 0010

Bul jerde xabar to'rt ha'r qi'yli' yekilik bloklar aji'rati'lg'an. Adresat woni' son'i'nan baslap sanap $r_2 + g = 7$ razryadtti' wo'shirip taslap 10101 aladi'. Buni' tekserip ko'remiz: 62199+13976+74879=151054.

Usi'g'an uqsas moduli ko'beytiw 75303 kriptotekstine qollani'p 33549 alami'z yamasa

33549=1000 0011 0000 1101

Wonda kiriwshi tekst 01100 boladi', yag'ni'y 7 razryadti' wo'shirip 5 razryadti' keri ta'rtipte alami'z.

A vektori' bloklarg'a aji'rati'lg'an tu'rde to'mendegishe boladi':

	$r_1 = 3$	$n = 5$	$g = 3$	$r_2 = 4$
$a_1 = 24717$	110	00001	000	1101
$a_2 = 20741$	101	00010	000	0101
$a_3 = 12808$	011	00100	000	1000
$a_4 = 9222$	010	01000	000	0110
$a_5 = 6157$	001	10000	000	1101

$r_1 = 3$ bolg'ani' menen ma'selede biz mu'mkin bolg'an ko'shiwlerdi yesapqa ali'p, da'slepki tosi'nnanli' kesindinin' uzi'nli'g'i'n 4 ke ten' dep aldi'q. Bul yekilik su'wretleniwlerde 16 razryad bar yekenligin an'latadi'. Bizin' mi'sali'mi'zda da'slepki segmenttin' maksimal uzi'nli'g'i' 5 ke ten'. Biraq adresat bug'an itibar bermese de boladi', soni'n' ushi'n woni'n' r_1 di biliwi za'ru'r yemes.

§ 5 Ti'g'i'z ryukzaklar

Ashi'q giltli kriptosistema tiykari'nda jati'rg'an ryukzak haqqi'ndag'i' ma'sele to'men ti'g'i'zli'qqa iye, yag'ni'y ryukzak vektori' komponentalari' 1 den *n* ge shekem kesindide ju'da' siyrek jaylasadi'. Bul paragrafta biz kriptosistema tiykari'nda jati'rg'an ryukzak vektori' ti'g'i'z yamasa joqari' ti'g'i'zli'qqa iye dep yesaplaymi'z.

Aldi'ng'i' paragraflarda biz a'dettegi yamasa modulyar arifmetikani' qollandi'q. Bul paragrafta bolsa shekli maydandag'i' arifmetika yamasa Galua maydani'ndag'i' arifmetikadan paydalanami'z.

Shekli maydan p^h elementlerden turadi', bunda p a'piwayi' san ha'm $h \geq 1$. Bunday tu'rdegi shekli maydan a'dette $F(p^h)$ dep belgilenedi.

Biz $F(p)$-tiykarg'i' maydandi', yag'ni'y 0,1,…, p-1 elementlerden turi'wshi' $F(p^h)$ maydani'ni'n' u'les maydani'n qarasti'rami'z. Tiykarg'i' maydanda p moduli boyi'nsha a'piwayi' arifmetika qollani'ladi'. Maydanda nolge ten' yemes ha'r bir elementtin' keri elemnti bar boladi'. Yegerde ha'm tek sonda g'an α elementi $F(p)$ maydani'nda $P(x)=0$ ten'lemesin qanaatlandi'rsa, wonda woni' $F(p)$ maydani' u'stinde h algebrali'q da'rejesi dep ataymi'z, bunda $P(x)$ - h da'rejeli ko'pag'zali'. $F(p^h)$ maydani'ni'n' barli'q p^h elementleri:

$$\sum c_j a^j, \quad 0 \leq c_j \leq p-1, \quad 0 \leq i \leq h-1$$

tu'rinde ko'rsetiliwi mu'mkin. yesaplawlardi' c_j «koefficentleri» p moduli boyi'nsha ali'nadi', al α^i , $i \geq h$, da'rejesi $P(\alpha) = 0$ ten'lemesin qollani'p kishi da'rejege almasti'ri'li'wi' mu'mkin.

Lemma 7. *Meyli p a'piwayi' ha'm* $h \geq 2$ *pu'tin san bolsi'n. wonda sondayda bir* $A = (a_1,....,a_p)$ *ryukzak vektori' bar boli'p wol to'mendegi sha'rtlerdi qanaatlandi'radi':*

(I) $1 \leq i \leq p$ *ushi'n* $1 \leq a_i \leq p^h - 1$

(II) *Meyli* $x_{i'}$ *ha'm* $y_{i'}$ *teris yemes pu'tin sanlar ha'm*

$$(x_1,...,x_p) \neq (y_1,...,y_p) \qquad (*)$$

bunda $\sum_{i=1}^{p} y_i = h$ *ha'm* $\sum_{i=1}^{p} y_i = h$. wonda

$$\sum_{i=1}^{p} x_i a_i \neq \sum_{i=1}^{p} y_i a_i \qquad (**)$$

Da'liylleniwi. $F(p^h)$ shekli maydani'n qarasti'rami'z. Meyli α - $F(p)$ dag'i' h da'rejeli algebrali'q element ha'm g - $F^*(p^h)$ gruppasi'ni'n' jasawshi'shsi' bolsi'n.

$$a_i = \log_g(\alpha + i - 1),\ 1 \leq i \leq p$$

ani'qlaymi'z. Bul jerde (I) sha'rt wori'nlanatug'i'ni' ko'rinip tur, sebebi wol a'piwayi' diskret logarifmnin' wo'zgeriw woblasti'n an'latadi'. (II) sha'rtin da'liyllew ushi'n keri tasti'yi'qlaw isleymiz: x_i ha'm y_i sanlari' tabi'ladi' ha'm wolar (*) sha'rtin qanaatlandi'radi', al (II) worni'na

$$\sum_{i=1}^{p} x_i a_i = \sum_{i=1}^{p} y_i a_i \qquad (**)'$$

alami'z. yegerde (**)' ten'ligin g da'rejege ko'tersek wonda ten'lik wori'nli' boli'p qaladi'. (**)" ten'lemesi

$$(\alpha+0)^{x1}....(\alpha+p-1)^{x_p} = (\alpha+0)^{y1}...(\alpha+p-1)^{y_p} \qquad (**)"$$

tu'rinde jazi'li'wi' mu'mkin. Bul ten'liktin' yeki ta'repin de α qarata ko'pag'zali' si'pati'nda jaza woti'ri'p, woni'n' yeki ta'repindegi α-n' joqari' da'rejeleri (*) sha'rti boyi'nsha sa'ykes boli'wi' kerek degen juwmaqqa kelemiz. Usi' sha'rtten bul joqarg'i' da'reje h qa ten' boltug'i'nli'g'i' kelip shi'g'adi'. (**)" shep

ta’repinen won’ ta’repin ali’p taslasaq u’lken da’rejesi $\le h-1$ bolg’an α den ali’ng’an nolge ten’ yemes ko’pag’zali’g’a iye bolami’z. Bunnan α da’rejesi $\le h-1$ bolg’an polinomial ten’lemeni qanaatlandi’radi’ ha’m sa’ykes tu’rde *h* da’rejeli algebrali’q element boli’wi’ mu’mkin yemes. Bul qarama-qarsi’li’q (**)' sha’rti wori’nlanbaytug’i’ni’n ko’rsetedi.

Yegerde p a’piwayi’ sanni’n’ da’rejesi bolg’an jag’dayda da da’liyllew usi’lay boladi’. Da’liyllewden (**) sha’rti qatan’ sha’rt penen almasti’ri’w mu’mkin:

$$\sum_{i=1}^{p} x_i a_i \neq \sum_{i=1}^{p} y_i a_i \pmod{p^h - 1}$$

Kriptosistemani’ du’ziwde kiriwshi tekst *p* razryadli’ bloklardan turi’p wolardi’n’ ha’r birinde ten’dey *h* birlik bar boladi’. Uli’wma aytqanda qa’legen yekilik ji’yi’nlardi’ bunday bloklarg’a aji’rati’wg’a bolmaydi’. Biraqta bloklardi’ da’slep talap yetilgen sha’rtti qanaatlandi’ratug’i’n ju’da’ uzi’n yekilik bloklar menen kodlaw mu’mkin. Buni’ to’mendegi lemmada ko’rsetemiz.

Lemma 8. *$h \ge 3$ ha’m $h < n$ natural sanlar bolsi’n. wonda* $\left[\log_2 \binom{n}{h}\right]$ *uzi’nli’qtag’i’ barli’q yekilik ji’yi’nlar ko’pliginin’ n uzi’nli’qtag’i’ barli’q usi’nday yekilik ji’yi’nlar ko’pligine jayi’lmasi’ bar boladi’.*

Da’liylleniwi. $\left[\log_2 \binom{n}{h}\right]$ uzi’nli’qqa iye yekilik ji’yi’nlardi’ *A* sani’ni’n’ yekilik ko’rinisi retinde qarasti’rami’z. Ha’r qaysi’si’ *h* birlikten turatug’i’n barli’q *n* uzi’nli’qtag’i’ ji’yi’nlardi’ alfavit boyi’nsha ta’rtiplestiremiz. Bul ta’rtiplestiriwdi yesapqa ali’p birinshi ji’yi’nda barli’q birlikler son’i’nda, al keyingi ji’yi’nda bolsa birlikler basi’nda jaylasadi’. *A* sani’n su’retlewshi yekilik ji’yi’ndi’ (*A*+1) ji’yi’ni’nda du’zilgen ta’rtiplesken dizimde ko’rseteyik. Bul

sa’wlelendiriwdin’ qaplama bolatug’i’nli’g’i’ bizge belgili. Biz dizimnin’ shegarasi’nan shi’g’i’p kete almaymi’z, sebebi wonda $\binom{n}{h}$ elementler, al x uzi’nli’qtag’i’ yekilik ji’yi’nlar bolsa bali’g’i’ boli’p 2^x ha’m wol $\binom{n}{h}$ asi’p ketpeydi, bunda $x = \left[\log_2 \binom{n}{h}\right]$.

Mi’sali’. N=5, h=2 bolsi’n, wonda $\left[\log_2 \binom{n}{h}\right] = 3$ ha’m bunnan biz uzi’nli’g’i’ 3 ke ten’ yekilik ji’yi’nlardi’ to’mendegishe kodlawi’mi’z mu’mkin: birinshi kolonkada uzi’nli’g’i’ 3 ke ten’ ji’yi’nlar, al yekinshide sa’ykes yeki birlikten turatug’i’n uzi’nli’g’i’ 5 ke ten’ ji’yi’nlar jazi’ladi’, yag’ni’y

000	00011
001	00101
010	00110
011	01001
100	01010
101	01100
110	10001
111	10010

Bul jerde 10100 ha’m 11000 ji’yi’nlari’ paydalani’lmaydi’. Yendi $n = 7$ ha’m $h = 2$ dep joqari’da islenege a’meller ja’rdeminde biz uzi’nli’g’i’ 4 ke ten’ barli’g’i’ boli’p tek 16 yekilik ji’yi’nlardi’ kodlawi’mi’z mu’mkin. Biraqta yeki birlikten turatug’i’n uzi’nli’g’i’ 7 ge ten’ yekilik ji’yi’nlar sani’ 21 ge ten’. To’mende inglis alfavitinin’ 21 ha’ribin kodlaw keltirilgen:

A	0000110	M	0100010
B	0000101	N	0100100
C	0000110	O	0101000
D	0001001	P	0110000
E	0001010	R	1000001
F	0001100	S	1000010
G	0010001	T	1000100
H	0010010	U	1001000
I’	0010100	V	1010000
K	0011000	W	1100000
L	0100001		

Biz bul ayti’lg’anlardi’n’ tiykari’nda kriptosistemani’ qarap wo’temiz. Da’slep $F(p^h)$ shekli maydanda diskret logarifmdi sheshiw mu’mkin bolatug’i’nday yetip p ha’m $h \le p$ a’piwayi’ sanni’n’ da’rjesin saylap alami’z.

Bunnan son’ $F(p)$ maydani’nda h da’rejesi bolg’an α algebrali’q elementin ja’nede $F^*(p^h)$ gruppasi’ni’n’ jasawshi’si’ bolg’an g saylap alami’z. (α, g) jubi’n saylawdi’n’ bir neshe variantlari’ bar. A’lbette α elementi $F(p^h)$ maydani’ni’n’ elementleri bergendegidey boli’wi’ sha’rt yemes. A’piwayi’li’li’q ushi’n biz sonday jag’day boli’p qaldi’ dep qabi’l yetemiz.

$$a_i = \log_g(\alpha + i - 1), \;\; 1 \le i \le p \qquad (*)$$

yesaplaymi’z. Bul sistemani’ du’ziwde tiykarg’i’ adi’m boli’p tabi’ladi’.

a_i sani’n, 1,...., p sanlari’n tosi’nnan ali’ng’an π wori’n almasti’ri’wlar menen aralasti’rami’z ha’m na’tiyjege saylap ali’ng’an $\forall d, 0 \le d \le p^h - 2$ ni’

$p^h - 1$ moduli boyi'nsha qosami'z. Meyli ali'ng'an vektordi' $B = (b_i, ..., b_p)$ dep belgileyik.

B, p ha'm h shifrlaw ushi'n ashi'q giltti quraydi'. Si'rli' lazeykani' α, g, π ha'm d du'zedi.

Meyli, yendi C - h birlikten turatug'i'n p uzi'nli'qqa iye yekilik ji'yi'n bolsi'n. Vektor-bag'ana si'pati'nda qarali'p ati'rg'an C vektori' $BC (\text{mod } p^h - 1)$ ni'n' yen' kishi won' qaldi'g'i' si'pati'nda shifrlanadi'.

Yegerde h, p g'a jaqi'n bolsa, wonda shifrlaw usi'g'anan uqsas ali'p bari'ladi'. Biraqta deshifrlaw Lemma 8 den kelip shi'g'adi'.

Si'rli' lazeykani' bilgen shaxs deshifrlaw ushi'n kriptoteksten hd ni' $p^h - 1$ moduli boyi'nsha ali'p taslaydi' ha'm y ti aladi'.

$F(p^h)$ maydani'nda g^y yesaplaymi'z. Wol da'rejesi $h-1$ den u'lken bolmag'an α qarata ko'pag'zali' boladi'. α wo'zgeriwshisi $\alpha^h = r(\alpha)$ ten'lemesin qanaatlandi'radi', bunda $r(\alpha)$ ko'pag'zali'ni'n' da'rejesi $h-1$ kishi.

$$s(\alpha) = \alpha^h + g^y - r(\alpha)$$

ko'pag'zali'si' $F(p)$ da ko'beytiwshilerge jiklenedi, sebebi $s(\alpha)$ ha'r bir da'reje ko'rsetkishi (*) tu'rinde bolg'an g da'reje ko'rsetkishlerinin' ko'beymesi boladi'. Kriptoteksten hd ali'p taslaw wog'an tosi'nnan d shamasi'ni'n' qosli'wi'ni'n' aldi'n aladi'. Ko'beymeler:

$$s(\alpha) = (\alpha + i_1 - 1)...(\alpha + i_h - 1)$$

Da'slepki tekstte birler ushi'n wori'ni' $i_1,....,i_h$ sanlari'na π^{-1}keri worni'na qoyi'wdi' qollang'annan son' ani'qlanadi'.

Da'slepki paragraflarda qaralg'an mi'sallarda bul algoritmdi qollana almaymi'z, sebebi wolardi' to'men ti'g'i'zli'qtag'i' ryukzaklar qollani'ldi'. Uli'wma jag'dayda $A=(a_1,...,a_n)$ ryukzak vektori'ni'n' ti'g'i'zli'g'i'

$$d(A)=\frac{n}{\log_2 \max A}$$

tu'rinde ani'qlanadi'. Tez wo'siwshi A vektori' ushi'n $a_n \geq 2^{n-1}$ ha'm sa'ykes $d(A) \leq n/(n-1)$. A'dette ti'g'i'zli'q tez wo'siwshi vektor jag'dayi'nda $n/(n-1)$ de to'men. Sebebi $\max A \geq n$ qa'legen ryukzak vektori' ushi'n ha'mme waqi'tta $d(A) \leq n/\log_2 n$. Mi'sali' $A=(1,2,3,.....128)$ ushi'n $d(A)=128/7=18.2857$.

Mi'sal: Meyli p=3, h=2 ha'm α - $x^2-x-1=0$ ten'lemsin qanaatlandi'rsi'n. $F(3^2)$ maydani'ni'n' elementlerin

$$0,1,2,\alpha,\alpha+1,\alpha+2,2\alpha,2\alpha+1,2\alpha+2$$

si'pati'nda an'lati'w mu'mkin. yesaplawlarda α joqari' da'rejelerin $\alpha^2=\alpha+1$ ja'rdeminde to'menletiw mu'mkin. Mi'sali'

$$(\alpha+2)(2\alpha+1)=2\alpha^2+5\alpha+2=2\alpha+2+5\alpha+2=\alpha+1$$

$F(p^h)$maydani'ni'n' $\beta \neq 0$ elementi ushi'n β^i qarasti'ri'wi'mi'z mu'mkin. $\beta^i=0$ yekenligi ani'q. Biraqta yeger $F(p^h)$ maydani'nda $i=1,2,,...,p^h-1$ da β^i da'rejeleri barli'q nolik yemes elemenlerin bolsa, wonda β ni' $F^*(p^h)$ (multiplikativ gruppa) maydani'ni'n' jasawshi'si' dep ataymi'z. Jasawshi'ni'

logarifmnin' tiykari' si'pati'nda qarasti'ri'w mu'mkin. Bunday logarifdi diskret logarifmler dep ataymi'z. yendi α barli'q da'rejelerin jazami'z:

i'	1	2	3	4	5	6	7	8
α^i	α	$\alpha+1$	$2\alpha+1$	2	2α	$2\alpha+2$	$\alpha+2$	1

Bul tablicadan α jasawshi' yekenligi ko'rinip tur. Tablicani' diskret logarifmler tablicasi' si'pati'nda da ko'rsetiw mu'mkin. woni'n' ushi'n joqarg'i' qatarda maydanni'n' ta'rtiplengen elementleri, al to'meninde jasawshi' elementtin' da'rejelerinin' ma'nisin jazami'z. Sonda

y	1	2	α	$\alpha+1$	$\alpha+2$	2α	$2\alpha+1$	$2\alpha+2$
$\log_\alpha y$	8	4	1	2	7	5	3	6

Bul logarifmler tablicasi' a'dettegi bo'liw ha'm ko'beytiw ushi'n da qollanami'z. Logarifmler p^h-1 moduli boyi'nsha ali'nadi'. Mi'sali'

$$\log_2(\alpha+2)(2\alpha+1)=\log_2(\alpha+2)+\log_2(2\alpha+1)=10=2$$

Bunnan $(\alpha+2)(2\alpha+1)=\alpha+1$ boladi'. Usi'g'an uqsas

$$\log_2((\alpha+1)/(2\alpha+1))=2-3=7$$

Bunnan $(\alpha+1)/(2\alpha+1)=\alpha+2$ boladi'.

$2\alpha+1$ elementi de $F^*(9)$ maydani'ni'n' jasawshi'si' boli'p tabi'ladi'.

y	1	2	α	$\alpha+1$	$\alpha+2$	2α	$2\alpha+1$	$2\alpha+2$
$\log_{2\alpha+1} y$	8	4	3	6	5	7	1	2

$\alpha+2$ ha'm 2α de maydanni'n' jasawshi'si' bolatug'i'ni'n an'sat tekseriw mu'mkin, bunnan basqa jasawshi'lar joq. Yegerde $\beta^i=1$ sha'rtin

qanaatlandi’ratug’i’n $i = p^h - 1$ yen’ kishi won’ da’reje bolsa, wonda β maydanni’n’ jasawshi’si’ boladi’. Sonli’qtan jasawshi’lar sani’ $\varphi(p^h - 1)$ ge ten’, bunda φ -Eyler funkciyasi’. Bizin’ mi’sali’mi’zda wol $\varphi(8) = 4$ ten’.

JUWMAQLAW

Bul pitkeriw qa’nignelik jumi’si’nda yen’ birinshi jarati’lg’an ashi’q giltli kriptosistema bolg’an ryukzak haqqi’ndag’i’ ma’selege tiykarlang’an ayi’ri’m sistemlar qarasi’ti’ri’ldi’.

Ryukzak haqqi’ndag’i’ ma’sele ashi’q giltli kriptosistema dep atali’wi’ni’n’ sebebi wonda mag’li’wmatlardi’ shifrlawda qollani’latug’i’n bazi’-bir intensiv wo’siwshi A vektori’na modulli’ arifmetika ja’rdeminde qosi’msha a’meller islenip B normal vektori’ ali’nadi’. Bul vektor mag’li’wmatlardi’ shifrlaw ushi’n ashi’q gilt wazi’ypasi’n atqaradi’. Yegerde izbe-izliktegi elementler sani’ az bolsa ha’m wol tez wo’siwshi bolmasa da ryukzak ma’selesin sheshiw qi’yi’n yemes yesaplanadi’. Haqi’yqati’nda ryukzak keminde 250 elementten turi’wi’ kerek degen talap qoyi’ladi’. Tez wo’siwshi izbe-izliktin’ ha’r bir ag’zasi’ni’n’ uzi’nli’g’i’ 200 ha’m 400 bit arali’g’i’nda, al modul uzi’nli’g’i’ bolsa 100-200 bitten ibarat boli’wi’ kerek degen sha’rt qoyi’ladi’.

Bul sha’rtler yesaplaw texnikasi’ni’n’ rawajlani’wi’ ha’m wolardi’n’ sekundi’na wori’nlaytug’i’n a’meller sani’ni’n’ ko’beyiwi, parallel programmalasti’ri’w texnologiyalari’ni’n’ rawajlani’wi’ ha’m sali’sti’rmali’ tu’rde tez algoritmlerdin’ payda boli’wi’ menen wo’zgeriwi mu’mkin.

Bunday tu’rdegi ryukzaklardi’ ku’sh isletip buzi’w mu’mkin yemes. Yegerde sekundi’na bir million variant tekseretug’i’n bolsa, wonda barli’q mu’mkin bolg’an ryukzak variantlari’n tekseriw ushi’n wog’an 10^{46} ji’l kerek boladi’. Bul woni’n’ a’meliy jaqtan mu’mkin yemes yekenligin ko’rsetedi.

Ryukzak haqqi’ndag’i’ ma’sele tiykarlang’an kriptosistemani’ bir neshe million kompyuterler yemes, al bir neshe kriptograflar ta’repinen a’melge asi’ri’wi’ mu’mkin. Ani’q bir sha’riyatlarda ryukzak ma’selesin buzi’w mu’mkin yekenligin SHamir ko’rsetti. Biraqta Martin-Xellman sistemasi’n uli’wma jag’dayda xesh kim buza almadi’. SHamir ha’m Cippel ta’repinen sistemadag’i’ tu’rlendiriwlerde ha’lsiz jeri tabi’li’p, wol normal izbe-izlikten ryukzakti’n’ tez wo’siwshi izbe-izligin tiklewge mu’mkinshilik berdi. Bul bayanatti’n’ na’tiyjeleri

konferenciyada Apple II kompyuterinde islep ko’rsetildi. Merkell-Xellman woriginal sxemasi’ ashi’lg’annan son’ ryukzak tiykari’ndag’i’ bir neshe sistemalar jarati’ldi’. Biraqta wolardi’n’ ko’pshiligi kriptografiyali’q usi’llar ja’rdeminde analizlenip buzi’ldi’. Usi’g’an uqsas Lu-Lee sistemasi’ha’m woni’n’ modifikaciyalari’, Goodman-McAuely, Pieprzyk ha’m moduli ryukzaklarg’a tiykarlang’an Niemi kriptosistemalari’ da bunday kriptografiyali’q usi’llarg’a qarsi’ tura almadi’. Ha’zirgi waqi’tta ryukzak algoritminin’ varianti’ bolg’an Char-Rivest ryukzak algoritmi qa’wpsiz dep sanaladi’.

Pitkeriw qa’nignelik jumi’si’nda ryukzak vektori’ni’n’ ha’r qi’yli’ tu’rleri ushi’n bir neshe mi’sallar islengen. Islengen mi’sallar tiykari’nda algoritm du’zilip Delphi tilinde programmasi’ islengen ha’m tiyisli na’tiyjeler ali’ni’p qosi’msha bo’liminde keltirilip wo’tken.

PAYDALANG'AN A'DEBIYATLAR

1. Salomaa A. Kriptografiya s otkri'ti'm klyuchom. M. «Mir». 1995 g. -318 s.
2. X.K.A. Van Tilborg. osnovi' kriptolgii. M. «Mir». 2006 g. -471 s.
3. B.YA.Ryabko., A.N.Fionov. Kriptograficheskie metodi' zashiti' informtscii.M. «Goryachaya liniya-Telekom» 2005 g. 229-s.
4. B.Shnayer. Prikladnaya kriptografiya. Protokoli', algoritmi' i isxodni'e teksti' na yazi'ke S. M. «Triumf». 2002 g.-616 s.
5. N. Smart. Kriptografiya. M. «Texnosfera» 2005 g.-529 s.
6. N. Koblic. Kurs teorii chisel i kriptografii. M. «TVP» 2001 g.-269 s.
7. Barichev S.G., Serov R.E. wosnovi' sovremnnoy kriptografii. M «Goryachaya liniya-Telekom» 2002 g. -152 s.
8. Xarin YU.S., bernik V.I., Matveev G.V. Matematicheskie osnovi' kriptologii. Mn.BGU, 1999 g -319 s.
9. Erosh I.L. Diskretnaya matematika. Matematicheskie voprosi' kriptografii. S-Pb. SPbGUPA, 2001 g. – 56 s.