КРИПТОНАЛИЗДЕ «СЫНАЎ» УСЫЛЫ ҲӘМ ОНЫҢ ЕСАПЛАЎ ҚУРАМАЛЫЛЫҒЫ

М.Қ. Бердимуратов, Ж.А. Нуруллаев
Қарақалпақ мәмлекетлик университети

Улыўма математикалық модели [3] де келтирилген айырым симметриялы криптосистеманы қараймыз.

Мейли, $X=(x_1,\ldots,x_n)\in A_N^n$ - шифрланыўы керек болған ашық текст; $\theta^0=\left(\theta_1^0,\theta_2^0,\ldots,\theta_L^0\right)\in\Theta\subseteq A_N^n$ - сол шифрлаў сеансында пайдаланған гилттиң ҳақыйқый мәниси; $f(\cdot)$ - криптографиялық түрлендириў; $Y=(y_1,y_1,\ldots,y_n)\in V_N^n$ - шифртекст (криптограмма):

$$Y=f(X;\theta^0) \tag{1}$$

Қәлеген криптосистеманың орынланыўы керек болған шәрти θ^0 гилттиң (параметр) белгиленген мәнисинде (1) түрлендириўдиң биективлилик шәрти болып, нәтийжеде

$$f^{-1}(Y;\theta^0)=X \tag{2}$$

шәрти орынланыўы керек.

(2) қатнас информацияны алыў ҳуқықына ийе ҳәм θ^0 гилтти билетуғын субъект тәрепинен дизимге алынған Y шифртексттиң шифрын ашыў алгоритмин анықлайды.

«Сынаў» (толық териў, «brute force attack») усылы (2) қатнасқа тийкарланып, оның мазмуны төмендегише:

1) Бар болған шифртекст $Y\in A_N^n$ ҳәм оған сәйкес келиўши $X\in A_N^n$ ашық текст тийкарында $\theta=(\theta_1,\theta_2,\ldots,\theta_L)$ ға қарата салыстырмалы теңлемелер системасы дүзиледи.

$$f^{-1}(Y;\theta)=x_i,\ i=\overline{1,n} \tag{3}$$

ямаса векторлы көринисте:

$$f^{-1}(Y;\theta^0)=X;$$

2) $\theta\in\Theta\subseteq A_N^n$ гилт параметриниң барлық мүмкин болған мәнислерин толық териў менен бул системаның L шешимлериниң $\Theta_0=\left\{\overline{\theta}^{(1)},\overline{\theta}^{(2)},\ldots,\overline{\theta}^{(l)}\right\}$ үлес көплиги табылады.

3) Егер табылған шешимлер саны $l=1$ болса, онда (2) ге муўапық $\theta=\theta^0$ параметриниң ҳақыйқый мәниси анықланады; кери жағдайда Θ_0 бир ноқатлы көплик болып есапланбайды ҳәм берилген параметр мәнислериниң l үлес

көплиги анықланып, (2) қатнасқа муўапық олардың ишинен биреўи θ^0 диң ҳақыйқый мәниси менен сәйкес келеди.

$l>1$ болған жағдайда (3) системада теңлемелер санын көбейтиў мақсетке муўапық. Буның ушын берилген X тийкарғы хабарында n символлар санын көбейтиў ямаса (3) де $q>1$ «хабар-шифртекст» жуплығын $(X^{(1)},Y^{(1)}),\ldots,(X^{(q)},Y^{(q)})$ алыў ҳәм пайдаланыў керек:

$$f^{-1}(Y^{(j)};\theta)=X^{(j)},\quad j=\overline{1,q} \tag{4}$$

n ҳәм q ларды арттырып, $l=1$ жағдайына ерисиў мүмкин ҳәм нәтийжеде гилтти қәтеликсиз баҳалай аламыз: $\overline{\theta}=\theta^0$.

Сүўретлениўден көринип турғанындай берилген көринистеги «сынаў» усылы A_2 (яғный, ашық ҳәм сәйкес шифртекстлерде) типиндеги криптоҳүжимлерде пайдаланады. «Сынаў» усылы айрым ўақытларда A_1 типиндеги криптоҳүжимлерде (тек шифртекстлар болғанда) пайдаланады; бунда (4) теңлик орнына барлық $\theta\in\Theta$ лер ушын « $f^{-1}(Y^{(j)};\theta)$ тексти «мәниске ийе ме» екенлиги тексериледи. Бирақ бундай қолланыў тек, узатылатуғын хабар алдыннан «мазмунға ийе текст» екенлиги белгили болғанда ғана мүмкин болады.

«Сынаў» усылының есаплаў қурамалылығы бул усылды иске асырыў ушын зәрүр компьютер әмеллериниң саны менен сыпатланады:

$$W=W(n,q,|\Theta|)=|\Theta|W_1(n,q) \tag{5}$$

бул жерде $|\Theta|$ - θ^0 параметри (гилт) ниң барлық мүмкин болған мәнислериниң саны $W_1(n,q)$ - θ дың бир мәниси ушын «сынаў» ға ((4) тексериўге) жумсалатуғын компьютер операциялары саны. Әдетте, $W_1(n,q)$ q дан сызықлы ғәрезли:

$$W_1(n,q)=w(n)q\,. \tag{6}$$

бунда $w(n)$ - $\theta\in\Theta$ бирлик мәнислери ушын n-символлы хабарларға қолланатуғын (3) ти тексериўге сарпланатуғын компьютер операциялары саны; $w(n)$ - гилт белгили болғанда шифртекстти шифрдан ашыўдағы ($f^{-1}(\cdot)$ кери функциясын есаплаў) компьютер операциялары саны менен сәйкес келеди. $w(n)$ шамасы ҳәр бир реал криптосистема ушын белгили характеристика болып, криптосистеманың тезлиги қанша жоқары болса, бул шама сонша киши екенлигин айтып өтиў орынлы [3].

(5) ҳәм (6) дан қаралып атырған криптоҳүжим усылы бойынша «сынаў» усылының есаплаў қурмалылығын ҳәм соның менен бирге берилген криптоҳүжим усылына қарата шифрлаў алгоритминиң криптотурақлылығын анықлайтуғын тийкарғы фактор $|\Theta|$ гилтлер кеңислигиниң қуўатлылығы

екенлиги келип шығады. Усыны есапқа алып белгили криптосистемалардың криптоанализи ушын «сынаў» усылының есаплаў қурамалылығын баҳалаймыз.

1. Алфавит символлары менен алмастырыў. Бул криптосистема ушын Θ - бул V_N алфавитиниң символлары менен мүмкин болған алмастырыўлар көплиги болып, оған тек бирдейликли алмастырыўлар кирмейди. Сонлықтан

$$|\Theta| = N!-1,\ W = (N!-1) = qw(n). \tag{7}$$

Айрым ўақытларда символлардың «араласыўын» күшейтиў ушын Θ ны жалғыз N максимал тәртиптеги циклға ийе моноцикллы алмастырыўлар көплиги сыпатында береди. Буннан

$$|\Theta| = (N-1)!,\ W = (N-1)!= qw(n). \tag{8}$$

екенлиги келип шығады.

2. Текст символларын T периоды менен орын алмастырыў. Бунда Θ -бул текст символларының орнын алмастырыўшы $\{1,2,\ldots,T\}$ индекслериниң барлық мүмкин болған алмастырыўлары көплиги болып, оған тек бирдейликли алмастырыўлар кирмейди. Сонлықтан

$$|\Theta| = T!-1,\ W = (T!-1) = qw(n). \tag{9}$$

(8) қатнастағыға уқсас, Θ моноцикллы алмастырыў жағдайында

$$|\Theta| = (T-1)!,\ W = (T-1)!= qw(n). \tag{10}$$

ға ийе боламыз.

(9) ҳәм (10) нан көринип турғанындай, текст символларын орын алмастырыў жәрдеминде шифрлаўда «сынаў» усылы менен криптоҳүжимниң есаплаў қурамалылығы (7) ҳәм (8) деги N алфавит қуўатлылығынан ғәрезли емес, ал T периоды шамасы менен анықланады.

3. Виженер шифры ҳәм оның модификациялары. Бул жағдайда

$$\Theta = \left\{\theta = (\theta_1, \theta_2, \ldots, \theta_T):\quad \theta_i \in V_N, i = \overline{1,T}\right\} \setminus \{0_T\},$$

сонлықтан,

$$|\Theta| = N^T - 1,\ W = (N^T - 1) = qw(n) \tag{11}$$

$T = 1$ де

$$|\Theta| = N - 1,\ W = (N - 1) = qw(n) \tag{12}$$

ушын Цезарь ҳәм Бофор шифрларын аламыз.

4. Вернама шифры (потоклы шифр). Буны $T = n$ болғанда яғный период шифрланатуғын текст

$$|\Theta| = N^n - 1,\ W = (N^n - 1) = qw(n) \tag{13}$$

узынлығы менен сәйкес болғанда Виженер шифрының дара жағдайы сыпатында қараў мүмкин.

5. DES блоклы-итерациялық шифр. Бул жағдайда екилик текст $(N = 2)$ $n = 64$ өлшемдеги блоклар менен шифрланады ҳәм 56 битли гилт пайдаланылады:

$$\Theta = \left\{\theta = (\theta_1, \theta_2, ..., \theta_{56}):\quad \theta_i \in V_2, i = \overline{1,56}\right\}$$

сонлықтан,

$$|\Theta| = 2^{56},\ W = 2^{56} qw(64) \tag{14}$$

DES тиң айрым арнаўлы қәсийетлеринен пайдаланып, W есаплаў қурамалылығын еки есе кемейтиў мүмкин.

6. IDEA блоклы-итерациялық щифр. Буның DES тен парқы гилт өлшеми 128 битке шекем үлкейтилген. Сонлықтан,

$$|\Theta| = 2^{128},\ W = 2^{128} qw(64) \tag{15}$$

7. ГОСТ 28147-89 блоклы-итерациялық щифр. Буның DES ҳәм IDEA дан парқы гилт өлшеми 256 битке шекем үлкейтилген. Сонлықтан,

$$|\Theta| = 2^{256},\ W = 2^{256} qw(64) \tag{16}$$

1-таблицада (7)-(16) формулалары жәрдеминде есапланған $|\Theta|$ ның мәнислери салыстырыў ушын келтирилген. Буннан тысқары айырым жийи қолланатуғын N, T, n параметрлериниң базыбир мәнислери ушын INTEL ASCI RED суперкомпьютери жәрдеминде $|\Theta|$ ны таңлаўдың орташа ўақтының мәниси (өсиў тәртибинде) келтирилген. Келтирилген санлардың әҳмийетин баҳалаў ушын, 70 жыллық адам өмириндеги секундлар муғдары шама менен $2{,}21 \cdot 10^9$ екенлигин келтирип өтемиз.

1-таблица

Гилтлер кеңислигиниң қуўатлылық сыпатламасы

Криптосистема	$\lvert\Theta\rvert$	INTEL ASCI RED ушын таңлаўдың орташа ўақты
Цезарь, $N = 26$	25	$1.2 \cdot 10^{-11}$ с
DES	$7.21 \cdot 10^{16}$	9.4 саат
Символларды моноцикллы алмастырыў $N = 26$	$1.55 \cdot 10^{25}$	$2.3 \cdot 10^6$ жыл
Символларды алмастырыў $N = 26$	$4.03 \cdot 10^{26}$	$6.0 \cdot 10^7$ жыл
IDEA	$3.40 \cdot 10^{38}$	$1.3 \cdot 10^{21}$ жыл

Виженер, $N = 26,\ T = 32$	$1.90 \cdot 10^{45}$	$7.3 \cdot 10^{27}$ жыл
ГОСТ 28147-89	$1.16 \cdot 10^{77}$	$1.7 \cdot 10^{58}$ жыл
Текст символларының Т – моноцикллы орын алмастырыўы, $T = 64$	$1.99 \cdot 10^{88}$	$2.9 \cdot 10^{69}$ жыл
Текст символларының Т – орын алмастырыўы, $T = 64$	$1.27 \cdot 10^{90}$	$1.9 \cdot 10^{71}$ жыл
Вернама (потоклы шифр) $N = 26,\ n = 128$	$1.30 \cdot 10^{181}$	$2.0 \cdot 10^{162}$ жыл

ПАЙДАЛАНЫЛҒАН ӘДЕБИЯТЛАР

1. Bauer F. Decrypted Secrets: methods and maxims of cryptology. N.Y.: Springer, 1997.
2. Молдовян Н.А. Проблематика и методы криптологии. СПб.: ИЗД-ВО СПбГУ,1998.
3. Харин Ю.С., Берник В.И., Матвеев Г.В., Агиевич С.В. Математические и компьютерные основы криптологии: МЗ4 Учеб. пособие - МН.: Новое знание, 2003. - 382 с.