Дәріс 8. Асимметриялық криптожүйелер

Жоспар:

1. Эль–Гамаль сұлбасы
2. Шнорр сұлбасы
3. Цифрлық қолтаңбаны қалыптастыру алгоритмі
4. Криптографиялық жүйені қалыптастыру алгоритмі

Эль-Гамаль криптожүйесі соңғы өрістердегі дискретті логарифмді есептеудің күрделілігіне негізделген. Ол үш негізгі кезеңді қамтиды: кілттерді құру, шифрлау және шифрды ашу.

Алгоритм кезеңдері:

1) p жай санын таңдаймыз;
2) біз екі кездейсоқ сандарды таңдаймыз $g, g < p$ және $x, x < p$
3) $y = g^x mod p$ есептейміз.

Эль–Гамаль схемасының ашық кілті y, g және p сандары, құпия кілті x саны болып табылады.

Сандық қолтаңбаны құру алгоритмі:

1) M хабары беріледі, оған қол қою керек;
2) $k, k < p$ кездейсоқ $p - 1$ өзара жай санын таңдаймыз;
3) келесіні есептейміз $a = g^k mod p$;
4) $M = (xa + kb) mod\ (p - 1)$ теңдеуден (4.8) формула арқылы b–ні анықтаңыз

$$b = (M - xa)k^{-1} mod(p - 1); \qquad (4.8)$$

5) қолтаңба қалыптастыру. Қолтаңба сандар жұбы (a, b) болып табылады.

k саны құпия кілт болып табылады.

Назар аударыңыз. Төртінші қадамда ЭЦҚ генерациялау кезінде M мәнінің орнына μ=H(M) мәнін пайдалануға болады, мұндағы H – хэш–функция.

Эль-Гамаль схемасындағы цифрлық қолтаңбаны тексеру келесідей:

1) M хабарламасы және (a, b) қолтаңба берілген.
2) есептейміз $y^a a^{\ b} mod\ p = [g^x]^a a^b = g^{xa} g^{xb} = g^{xa=xb} = g^M mod p$;
3) $g^M\ mod\ p$ есептейміз;

Егер мәні келесідей болса $y^a a^{\ b} mod\ p$ мәні $g^M\ mod\ p$ сәйкес келсе, онда қолтаңба дұрыс.

Шифрды шешу алгоритмі 1:

1) M хабарлама берілді;
2) $p - 1$ өзара жай санымен кездейсоқ $k, k < p$ санын таңдаймыз;
3) $a = g^k mod p$ есептейміз;
4) хабарламаны (4.9) формула арқылы шифрлаймыз

$$b = y^k M \bmod p = g^{kx} M \bmod p. \quad (4.9)$$

Хабар жұбы (a, b) шифрлық мәтін болып табылады. Бұл шифрлау әдісі бар шифрлық мәтін бастапқы мәтіннен ұзағырақ екенін ескеріңіз.

Кері шифрлау алгоритмі 2:

1) $ax \equiv g^{kx} \bmod p$ есептейміз

2) Онда $M = b/a^x \equiv g^{kx} M / g^{kx} \bmod p.$

Шнорр сұлбасы

Шноррдың криптографиялық схемасы-дискретті логарифмді есептеудің күрделілігіне негізделген цифрлық қолтаңба схемасы. Ол үш кезеңнен тұрады: кілттерді құру, қолтаңба жасау және қолтаңбаны тексеру. Шнорр схемасы келесідей орындалады:

Шнорр сұлбасын қалыптастыру алгоритмі

1) p және q екі жай сандарын таңдаңыз, сонда q көбейткіш болады $(p - 1)$;

2) a мәнін таңдаңыз, Бұл $a \neq 1$ және $a^q \equiv 1 \bmod p$;

3) кездейсоқ санды таңдаңыз $s, s < q$.

4) $y = a^{-s} \bmod p$ есептеңіз.

Шнорр сұлбасының ашық кілті–p, q және a сандары. Құпия кілт – y саны.

Шнорр схемасы дискретті логарифм мәселесінің күрделілігіне негізделген. Шнорр схемасын жүзеге асыру үшін p және q сияқты екі жай сан таңдалады, осы жағдайда келесі мәндер орын алады $(q|p - 1)$ – q – ді $p - 1$–ге бөледі. Әрі қарай p модулі бойынша шегерімдер класына жататын сандар жиынтығының ішінен $p, p \in Z_p$, келесідей g санын таңдалынады

$$g^q = 1 \bmod p.$$

q, p, g сандары Шнорр схемасының ашық параметрлері болып табылады. Схеманың жеке кілті үшін ерікті бүтін сан таңдалады $x, 1 \leq x \leq q - 1$, және сан есептеледі (ашық кілт)

$$y = g^{-x}.$$

Шнор сұлбасының аутентификациян орындау үшін келесі қадамдар орындалады:

1–қадам. *A* пайдаланушысы $k, 1 \leq k \leq q - 1$ санын таңдайды және есептейді

$$r = g^k \bmod p.$$

2–қадам. *A* қатысушысы *r* нөмірін *B* пайдаланушысына жібереді.

3–қадам. *В* қатысушысы $e, 0 \leq e \leq 2^t - 1$санын таңдайды, мұндағы t – кейбір параметр және бұл санды *А* жағына жібереді.

4–қадам. *А* пайдаланушысы (6.1) формуласы бойынша есептейтін *В* нөмірін s жібереді:

$$s = k + xe. \tag{8.1}$$

5–қадам. *В* қатысушысы санды есептейді

$$r' = g^s y^e \bmod p.$$

Егер r' саны бірінші қадамдағы r санына сәйкес келсе, онда *В* қатысушыға *А* сенеді, әйтпесе, *В* қатысушы *А* қатысушысын қабылдамайды.

Шнорр сұлбасы тиімділігі мен қауіпсіздігінің жоғары деңгейіне байланысты заманауи криптографиялық жүйелерде кеңінен қолданылады. Ол пайдаланушылардың аутентификациясы, құжаттарды қорғау және электрондық хабарламалар үшін цифрлық қолтаңбаларда қолданылады. Биткоин сияқты криптовалюталарда Шнорр схемасы транзакцияларға қол қою үшін қолданылады, олардыңностьамдылығын қамтамасыз етеді және өңдеу процесін жылдамдатады. Сондай-ақ, бұл алгоритм деректерді қорғау жүйелерінде, банктік қызметтерде және ақпараттың түпнұсқалығын сенімді тексеру қажет мемлекеттік құрылымдарда қолданылады. Шамдық пен жылдамдықтың арқасында Шнорр схемасы криптографиялық қорғаудың перспективалы әдістерінің бірі болып табылады.

Цифрлық қолтаңбаны қалыптастыру алгоритмі

Сандық қолтаңба алгоритмі деректердің түпнұсқалығын тексеруге және олардың өзгермейтіндігін растауға арналған. Ол үш негізгі кезеңнен тұрады: кілттерді құру, қолтаңба жасау және қолтаңбаны тексеру. Цифрлық қолтаңбаны қалыптастыру алгоритмі келесідей орындалады:

1) M хабарламасы және $H(M)$ хэш функциясы берілген;

2) кездейсоқ $r, r < q$ санын таңдаңыз;

3) $x = a^r \bmod p$ есептеңіз;

4) M хабарламасына x мәнін қосып, $e = H(M, x) \bmod q$ есептеңіз;

5) $v = (r + se) \bmod q$ мәнін есептеңіз;

6) біз қолтаңба жасаймыз. Қолтаңба сандар жұбы (e, v).

Назар аударыңыз. r саны–құпия сан.

Қолтаңбаны тексеру:

1) M хабарламасы және (e, v) қолы берілген;

2) $x^1 = a^v y^e \bmod p$ мәні есептеледі, мұндағы $a^v y^e = a^{(e+se) \bmod q} a^{-se \bmod q} = a^y$;

3) M хабарламасына x^1 мәнін қосып, есептеңіз: $e^1 = H(M, x^1) \bmod q$;

4) Егер $e^1 = e$ болса, онда қолтаңба дұрыс деп саналады.

Назар аударыңыз. 2 – тармақта қолданылатын r және s сандары жеке

кілттер болып табылады. Олар тек есептеуді тексеру үшін қолданылады.

Аутентификация хаттамасы:

1) *A* жіберуші және *B* қабылдағыш бар;

2) *A* пайдаланушысы кездейсоқ $r, r < q$ санын таңдап, есептейді

$$x = a^r mod\ p;$$

3) *A* пайдаланушысы *B* санын x жібереді;

4) B пайдаланушысы $[0, 2^t - 1]$диапазонынан кездейсоқ e санын таңдайды;

5) *B* пайдаланушысы *A* нөмірін e жібереді;

6) *A* пайдаланушысы есептейді

$$v = (r + se)\ mod\ q;$$

7) *A* пайдаланушысы *B* нөмірін v жібереді;

8) B пайдаланушысы $x = a^v y^e\ mod\ p$ есептейді, мұндағы $a^v y^e = a^{(e+se) mod\ q} a^{-se\ mod\ q} = a^y$;

9. Егер x_1 = *x* болса, онда аутентификация дәлелі қабылданады.

Ескерту. Аутентификация хаттамасында кездейсоқ сан e – ЭЦҚ-дан айырмашылығы *B* алушы анықтайды.

Назар аударыңыз. Аутентификация алгоритмінің қауіпсіздігі t параметріне байланысты. Шнорр 512 бит ретті p мәнін, 140 биттік q және 72–ге тең t мәнін пайдалануды ұсынады.

Рюкзак есебін қарастырайық және осы есептің негізінде біз ашық кілтті криптографиялық жүйені құрастырамыз.

Рюкзак мәселесі. Берілген жиын (вектор)

$$A = (a_1, a_2, \ldots, a_n),$$

n натурал сан және бір натурал V саны. Қосындысы V–ге тең, мүмкін болса, $a_i,\ i = 1, 2, \ldots, k$ сандарын табу керек. Қарапайым жағдайда V санының өлшемін көрсетеді. рюкзак және $i = 1, 2, \ldots, k$ сандарының әрқайсысы рюкзакқа салуға болатын заттың өлшемін көрсетеді. Міндеті бойынша рюкзак толығымен толтырылған нысандардың жиынтығын табу болып табылады.

Көрсеткіш ретінде мысал келтіреміз.

3231 және 10 сандар жиынтығы 43, 129, 215, 473, 903, 302, 561, 1165, 697, 1523 сандарды қарастырайық.

Байқасақ, бұл 3231 = 129 + 473 + 903 + 561 + 1165. Нәтижесінде біз қажетті шешімді таптық.

Негізінде, шешімді әрқашан *A* ішкі жиындарын толығымен санау және олардың қосындыларының қайсысы *V*-ге тең екенін тексеру арқылы табуға болады. Біздің жағдайда бұл бос жиынды қосканда $2^{10} = 1024$ ішкі жиынды санауды білдіреді. Бұл толығымен орындалады.

Алайда, егер $n = 300$ болса, онда бұл жағдайда 2^{300} ішкі жиындардың арасынан іздеу керек, бұл проблемалық тапсырма. 2^{300} ішкі жиын арасында іздеуді өңдеу мүмкін емес.

n өлшемді A векторын пайдаланып, $f(x)$ функциясын төмендегідей анықтауға болады. $0 \leq x \leq 2^n - 1$ интервалындағы кез келген x санын n биттің екілік көрінісі арқылы анықтауға болатынын ескеріңіз, мұнда қажет болған жағдайда $(2^n - 1)$ кіші сандар үшін жоғары ретті биттер алдыңғы нөлдер қосылады.

Олай болса, $0 \leq x \leq 2^n - 1$ аралығындағы x санының екілік кескіні келесі түрге ие болсын

$$x = x_1 x_2 \ldots x_n,$$

мұндағы $x_i \in \{0,1\}$;2yt $i = 1, 2, \ldots, n$. Содан кейін әрбір x мәні келесі (4.10) формула арқылы S санымен байланыстырылады

$$f(x) = x_1 a_1 + x_2 a_2 + \ldots + x_n a_n = S. \qquad (4.10)$$

Екі вектордың скаляр көбейтіндісін пайдаланып жаза аламыз.

$f(x) = A\,x$ мұндағы A және x – n өлшемді векторлар. Енгізілген функцияны пайдалану $f(x) = A\,x$, алдыңғы теңдік $3231 = 129 + 473 + 903 + 561 + 1165$ келесі түрде жазуға болады

$$0 * 43 + 1 * 129 + 0 * 215 + 1 * 473 + 1 * 903 + 0 * 302 + \\ +1 * 561 + 1 * 1165 + 0 * 697 + 0 * 1523 = \\ = f(0101101100) = \\ = f(364) = 129 + 473 + 903 + 561 + 1165 = 3231,$$

өйткені 0101101100 екілік саны ретінде ұсынылуы мүмкін

$$0101101100 = 0 * 10^9 + 1 * 10^8 + 0 * 10^7 + 1 * 10^6 + \\ +1 * 10^5 + 0 * 10^4 + 1 * 10^3 + 1 * 10^2 + 0 * 10^1 + 0 * 100 = \\ = 0 * 29 + 1 * 28 + 0 * 27 + 1 * 26 + 1 * 25 + 0 * 24 + 1 * 23 + 1 * 22 + 0 \\ * 21 + 0 * 20 \\ = 0 + 1 * 256 + 0 + 1 * 64 + 1 * 32 + 0 + 8 + 4 + 0 + 0 \\ = 256 + 64 + 32 + 8 + 4 = 364.$$

$f(x)$ мәнінен x мәнін анықтау қиын екенін ескеріңіз. Алайда, егер біз x-ті $f(x)$-тан қалпына келтіре алсақ, онда x санының екілік көрінісінен $f(x)$ үшін қосындыға кіретін A жиынының құрамдастарын анықтай аламыз. Екінші жағынан, x-тен $f(x)$ есептеу оңай. Бұдан шығатыны, сөмке мәселесі бір жақты функция үшін жақсы үміткер болып табылады. Әрине, біз n санының жеткілікті үлкен болуын талап етуіміз керек, айталық, кем дегенде 200. Төменде біз $f(x)$ функциясын пайдаланып құпиясы бар бір жақты функцияның

аналогын қалай анықтауға болатынын көрсетеміз. Осылайша, ашық кілтпен кейбір криптографиялық жүйені құрастырыңыз.

Алдымен, «рюкзак векторлары» A криптожүйенің негізі ретінде қалай пайдалануға болатынын қарастырайық. Немесе басқаша, A тізбегін пайдаланып бастапқы мәтінді шифрлық мәтінге қалай түрлендіру керек. Тапсырма шеңберінде біз келесі шифрлау схемасын құрастыра аламыз:

1) кезектілігі анықталады $A = (a_1, a_2, \dots, a_n)$;

2) бастапқы мәтін екілік реттілікке түрлендіріледі;

3) Екілік реттілік әрқайсысы n биттен тұратын блоктарға бөлінген, мұндағы n мәні A жиынындағы элементтер саны;

4) Ағымдағы бастапқы $x_1\, x_2 \dots x_n$ блок n бит (4.11) формула арқылы шифрланады

$$C = x_1 a_1 + x_2 a_2 + \dots + x_n a_n, \qquad (4.11)$$

мұндағы C бастапқы мәтіннің ағымдағы блогының шифры $x_1\, x_2 \dots x_n$.

Егер сіз компьютерлерді шифрлау үшін қолдансаңыз, онда компьютер жадында барлық шығарылатын ақпарат автоматты түрде екілік реттілік түрінде ұсынылатындығын ескеріңіз. Сондықтан ақпаратты екілік реттілік түрінде ұсыну қосымша түрлендіруді қажет етпейді.

Рюкзак мәселесіне негізделген ашық кілтті криптожүйені құру идеясы тиімді шешуге болатын рюкзак тапсырмалар класын құру болып табылады. Мұндай тапсырмалардың осы класы үшін оларды жалпы жағдайға өзгертетін параметрлерді түрлендіру бар. Бастапқы тапсырмалардың параметрлері криптографиялық жүйенің құпия кілтін анықтайды, ал өзгертілген тапсырманың параметрлері ашық кілтті құрайды. 1978 жылы тез өсетін $A = (a_1, a_2, \dots, a_n)$ тізбегі бар рюкзак мәселесі оңай шешілетін мәселе ретінде ұсынылды.

Анықтама. Барлық j үшін $0 \le j \le n$ болса, n саннан тұратын жиын (тізбегі) жылдам өсетін деп аталады.

$$a_j > a_1 + a_2 + \dots + a_{j-1}.$$

Жылдам өсіп келе жатқан сандар жиынтығы бар рюкзак мәселесі жалпы жағдайға қарағанда әлдеқайда оңай. Бұл жағдайда шешімді табу үшін A жиынтығын оңнан солға қарай бір рет қарап шығу жеткілікті, мүмкін нұсқалардың толық таңдауын орындамау керек. Шешімді іздеу алгоритмін келесідей сипаттауға болады:

– Берілген V үшін рюкзак немесе шифрланған *x* жиынының өлшемі және $j = n$ индекс мәні үшін алдымен $V < a_j$ теңсіздігін тексереміз. Егер $V < a_j$ болса, онда a_j қажетті сомаға қосу мүмкін емес.

– Егер $V < a_j$ болса, онда a_j қосындыға қосылуы керек. Бұл қалған a_j қосындысы *V*-ден аз болатынынан шығады. Бұл дәлелдеуді келесі есептеу (4.12) формулаларына келтіруге болады. Берілген V және j индексі үшін

формулалар арқылы x_j анықтаймыз

$$x_j = 1, \text{ егер } V \geq a_j \; x_j = 0, \text{ егер } V < a_j. \qquad (4.12)$$

Әрі қарай V және j жаңа мәнді келесі түрде есептейміз

$$V = V - x_j * a_j, j = j - 1.$$

Содан кейін $j = n - 1, n - 2, \ldots, 1$ үшін осы процедураны қайталаймыз.

Енді біз тез өсетін реттілікпен рюкзак мәселесін шешу алгоритмін құрастыра аламыз.

1) Жылдам өсетін жиынтықты $A = (a_1, a_2, \ldots, a_n)$ және V санын анықтау;
2) $j = n, n - 1, \ldots, 1$ үшін 3-5 қадамдары орындалады;
3) Егер $V \geq a_j$, онда $x_j = 1$, әйтпесе $x_j = 0$;
4) $V = V - x_j * a_j$ есептелінеді;
5) j теңдігін $(j - 1)$ орнатылды;
6) 2–ші қадамға қайтамыз.

Тұжырымдалған алгоритм кез келген V үшін рюкзак мәселесінің ең көп дегенде бір шешімі бар екенін көрсетеді, егер A жылдам өсетін тізбек болса.

Осылайша, егер A-тез өсетін реттілік болса, онда кез келген екілік реттіліктен V мәнін оңай есептеуге болады. Демек, егер тез өсіп келе жатқан A жиынтығы ашық болса, онда заңсыз пайдаланушы мәтінді заңды сияқты оңай шеше алады.

$$A = (a_1, a_2, \ldots, a_n)$$

кейбір жиынтықта

$$B = (b_1, b_2, \ldots, b_n).$$

Осылайша, B тізбегі тез өспейтін және рюкзактың ерікті векторына ұқсайтын етіп жиынтықты өзгерту керек. Бұл жағдайда B жиынтығы A-ның тез өсіп келе жатқан тізбегін қолдана отырып, оны қолдана отырып шифрланған мәтінді шешуге мүмкіндік беретін қасиетке ие болуы керек.

Криптографиялық жүйені қалыптастыру алгоритмі

1) Жылдам өсетін жиынтықты анықтау

$$A = (a_1, a_2, \ldots, a_n);$$

2) m модулін келесі теңсіздік орындалатындай етіп таңдаңыз:

$$m > S = a_1 + a_2 + \ldots + a_n;$$

3) m-ге салыстырмалы жай болатын t бүтін кездейсоқ санды (көбейткіш) таңдаймыз.

4) t^{-1} санын t-ге кері есептейміз, яғни келесідей орын алады

$$tt^{-1} \equiv 1 \, mod \, m.$$

5) $A = (a_1, a_2, ..., a_n)$ жиынынан жиынды есептейміз

$$B = (b_1, b_2, \ldots, b_n)$$

(4.13) формула арқылы

$$b_j = ta_j, 0 \leq j \leq n. \qquad (4.13)$$

Осылайша, белгілі бір B жиынтығы, рюкзак мәселесіне негізделген криптографиялық жүйе үшін шешуші болып табылатын, жылдам өсіп келе жатқан A жиынын «маскалайды».

Рюкзак мәселесіне негізделген бұл криптографиялық жүйенің ашық кілті $B = (b_1, b_2, ..., b_n)$ тізбегі болып табылады. B векторының көмегімен хабарламаның бастапқы мәтіні шифрланады. Жүйенің құпия кілті жылдам өсетін $A = (a_1, a_2, \ldots, a_n)$ жиынын m модулін және $t(t^{-1})$ санын қамтитын параметрлер болып табылады.

Назар аударыңыз. Құрылған криптографиялық жүйенің сенімділігін арттыру үшін алдымен A жиынын реттілік элементтерінің кейбір кездейсоқ таңдалған алмастырулары арқылы түрлендіруге болады. Бұл жағдайда кездейсоқ таңдалған ауыстыру құпия кілтке кіретін параметр болып табылады.

Ендеше, келесідей

$$C = c_1 + c_2 + ... + c_n$$

шифрленген мәтін блогы бар $c_i = x_i b_i, 0 \leq i \leq n$. Келесі ереже бойынша C таңдайық

$$C = x_1 b_1 + x_2 b_2 + ... + x_n b_n \equiv$$
$$\equiv x_1 t a_1 + x_2 t a_2 + ... + x_n t a_n.$$

Содан кейін шифрды шешу алгоритмі келесідей тұжырымдалады:

1) V саны есептеледі

$$V \, mod \, m \equiv t^{-1} C \, mod \, m \equiv$$

$$\equiv t^{-1}c_1 + t^{-1}c_2 + \ldots + t^{-1}c_n \, mod \, m \equiv$$
$$\equiv x_1 t^{-1} t a_1 + x_2 t^{-1} t a_2 + \ldots + x_n t^{-1} t a_n \, mod \, m \equiv$$
$$\equiv x_1 a_1 + x_2 a_2 + \ldots + x_n a_n \, mod \, m;$$

2) *V* мәнін анықтау үшін біз тез өсетін $A = (a_1, a_2, \ldots, a_n)$ жиынтығы үшін рюкзак мәселесін шешеміз.

Мысал. Рюкзак мәселесі негізінде криптографиялық жүйені қалыптастыру.

1) тез өсетін жиынтықты анықтаңыз

$$A = (1, 3, 5, 11, 21, 44, 87, 175, 349, 701);$$

2) Есептеу

$$S = 1 + 3 + 5 + 11 + 21 + 44 + 87 + 175 + 349 + 701 = 1397;$$

3) $m, m = 1590 > S = 1397$модулін таңдаңыз;

4) m мен өзара қарапайым $t = 43$ бүтін кездейсоқ санды таңдаңыз;

5) t^{-1} санының t–ге кері мәнін есептеңіз, яғни $tt^{-1} \equiv 1 \, mod \, m$.

Салыстыру шешімі $43x \equiv 1 \, mod \, 1590$ формуламен анықталады

$$x \equiv t^{-1} \equiv (-1)^{-1} P_{k-1} mod \, 1590,$$

мұндағы k мәні m/a бөлшегін сәйкес фракциялар тізбегіне ыдыратудағы кеңейтілген Евклид алгоритміндегі қадамдар саны. Біздің жағдайда $a = 43$ және $m = 1590$; P_{k-1} кеңейтілген Евклид алгоритмін қолдана отырып, a/m бөлшегінің ыдырауындағы соңғы сәйкес бөлшектің алымы.

Естеріңізге сала кетейік, Евклид алгоритміндегі қолайлы бөлшектердің нумераторлары (4.14) формуласы бойынша есептеледі

$$Pi = qi \times Pi - 1 + Pi - 2, \qquad i = 1, 2, \ldots, k, \qquad (4.14)$$

мұндағы $P_0 = 1$, $P_1 = q_1$ – бастапқы P_i мәндері; q_i – a және m сандары үшін ЕҮОБ есептеу кезінде Евклид алгоритміндегі бөліктер. біздің жағдайда a = 43 және m = 1590.

Сонымен, салыстыру шешімі үшін $43x \equiv 1 \, mod \, 1590$ келесі қадамдарды орындаңыз:

1) біз q_1–ді a = 43 және m = 1590 бөлінуінің бөлігі ретінде анықтаймыз. Біз q_1=36 аламыз. r_2=42 бөлінуінің қалдық мәні. Содан кейін анықтама бойынша P_0=1, P_1=q_1= 36;

2) a = 43 санын алдыңғы r_2 = 42 қалдығына бөлуден q_2 және r_3 қалдығын есептеңіз. Біз q_2=1 және r_3=1. аламыз. Содан кейін, анықтама бойынша

$$P_2 = q_2P_1 + P_0 = 1 \times 36 + 1 = 37;$$

3) алдыңғы бөліктің бөлінуінен q_3 бөлігін және r_4 қалдығын есептеңіз q_2=1 қалған $r_3 = 1$. Біз $q_3 = 1$, ал қалған $r_4 = 0$ аламыз;

4) қалдық $r_4 = 0$ болғандықтан, Эвклидтің кеңейтілген алгоритмі бойынша есептеу процесі аяқталады. Бұл өз кезегінде (4.15) формула бойынша мүмкіндік береді

$$x \equiv t^{-1} \equiv (-1)^{-1}P_{k-1} \, mod \, 1590 \qquad (4.15)$$

Салыстыру шешімін анықтаңыз $43x \equiv 1 \, mod \, 1590$, ол $x \equiv t^{-1} \equiv (-1)^{k-1}P_{k-1} mod \, 1590 \equiv (-1)^2 37 \, mod \, 1590 \equiv 37 \, mod \, 1590$ тең.

Шынында да, $43 \times 37 = 1591 \equiv 1 \, mod \, 1590$. Осылайша, $t = 43$ параметрін орнатып, оған кері элементті анықтағаннан кейін $t^{-1} = 37$, біз рюкзак мәселесін қолданатын криптографиялық жүйені құруды жалғастырамыз. Ол үшін біз криптографиялық жүйені қалыптастыру алгоритмінің 5-қадамына өтіп, жылдам өсіп келе жатқан $A = (1, 3, 5, 11, 21, 44, 87, 175, 349, 701)$ векторын «бүркемелейтін» векторды есептеуіміз керек.

5. B жинағын есептейміз $B = (b_1, b_2, \ldots, b_n$, ол (4.16) формула бойынша жылдам өсетін A векторын бүркемелейді:

$$b_j \equiv ta_j \, mod \, 1590, 0 \leq j \leq n. \qquad (4.16)$$

Алынады:

$$b_1 \equiv 43 \bullet 1 \, mod \, 1590 \equiv 43,$$
$$b_2 \equiv 43 \bullet 3 \, mod \, 1590 \equiv 129,$$
$$b_3 \equiv 43 \bullet 5 \, mod \, 1590 \equiv 215,$$
$$b_4 \equiv 43 \bullet 11 \, mod \, 1590 \equiv 473,$$
$$b_5 \equiv 43 \bullet 21 \, mod \, 1590 \equiv 903,$$
$$b_6 \equiv 43 \bullet 44 \, mod \, 1590 \equiv\equiv 1892 \equiv (1590 + 302) \, mod \, 1590 \equiv \equiv 302,$$
$$b_7 \equiv 43 \bullet 87 \, mod \, 1590 \equiv 3741 \equiv (2 \bullet 1590 + 561) \, mod \, 1590 \equiv \equiv 561,$$
$$b_8 \equiv 43 \bullet 175 \, mod \, 1590 \equiv 7525 \equiv (4 \bullet 1590 + 1165) \, mod \, 1590 \equiv \equiv 1165,$$
$$b_9 \equiv 43 \bullet 349 \, mod \, 1590 \equiv 150007 \equiv (9 \bullet 1590 + 697) \, mod \, 1590 \equiv \equiv 697,$$
$$b_{10} \equiv 43 \bullet 701 \, mod \, 1590 \equiv 30143 \equiv (18 \bullet 1590 + 1523) \, mod \, 1590 \equiv \equiv 1523.$$

Нәтижесінде келесі B жиынтығы алынды

$$B = (43, 129, 215, 473, 903, 302, 561, 1165, 697, 1523).$$

Сонымен, біз ақпаратты шифрлауға арналған $B = (43, 129, 215, 473, 903, 302, 561, 1165, 697, 1523)$ ашық жиыны бар сөмке мәселесіне негізделген криптографиялық жүйені және мәтінді шешуге арналған құпия параметрлерді құрдық. Бұл құпия параметрлерге тез өсіп келе жатқан жиынтық кіреді:

1) $A = (1, 3, 5, 11, 21, 44, 87, 175, 349, 701)$;

2) $m = 1590$ модулі;

3) $t = 43$ мультипликаторы және $t^{-1} = 37$ мультипликаторына кері;

4.7 Мәтінді шифрлау сұлбасы

Шифрлауды қажет ететін «*Добро ори клон»* хабарлама берілсін. Хабарламаға енгізілген таңбалардың ұзындығы бес биттік келесі екілік кодтары бар деп есептейік.

СИМВОЛ	**КОД**
Бос орын	00000
Д	10011
О	00001
Б	10101
Р	01110
И	00100
К	01000
Л	00101
Н	01100.

Бұл кодтар үшін бастапқы хабарлама келесі екілік реттілікке түрлендіріледі

1001100001 1010101110 0000100000
0000101110 0010000000 0100000101
0000101100.

Екілік тізбекті 10 биттен тұратын жеті блокқа бөлеміз:

1001100001
1010101110
0000100000
0000101110
0010000000
0100000101
0000101100

Биттер саны B жиынындағы элементтер санымен анықталады. Әрбір блок шын мәнінде екі хабарлама таңбасының шифры болып табылады және келесі ондық сандарға сәйкес келеді

$$1001100001 =$$

$$= 1 * 2^9 + 0 * 2^8 + 0 * 2^7 + 1 * 2^6 + 1 * 2^5 + 0 * 2^4 + 0 * 2^3 + 0 * 22 + 0 * 2 + 1 * 20 = 512 + 0 + 0 + 64 + 32 + 0 + 0 + 0 + 0 + 1 = = 609,$$

$$1010101110 = 1 * 2^9 + 0 * 2^8 + 1 * 2^7 + 0 * 2^6 + 1 * 2^5 + 0 * 2^4 + 1 * 2^3 + 1 * 2^2 + 1 * 2 + 0 * 20 = 512 + 0 + 128 + 0 + 32 + 0 + 8 + 4 + 2 + 0 = 686,$$

$$0000100000 = = 0 * 2^9 + 0 * 2^8 + 0 * 2^7 + 0 * 2^6 + 1 * 2^5 + 0 * 2^4 + 0 * 2^3 + 0 * 2^2 + 0 * 2 + 0 * 20 = 0 + 0 + 0 + 0 + 32 + 0 + 0 + 0 + 0 + 0 = 32,$$

$$0000101110 = = 0 * 2^9 + 0 * 2^8 + 0 * 2^7 + 0 * 2^6 + 1 * 2^5 + 0 * 2^4 + 1 * 2^3 + 1 * 2^2 + 1 * 2 + 0 * 20 = 0 + 0 + 0 + 0 + 32 + 0 + 8 + 4 + 2 + 0 = 46,$$

$$0010000000 = = 0 * 2^9 + 0 * 2^8 + 1 * 2^7 + 0 * 2^6 + 0 * 2^5 + 0 * 2^4 + 0 * 2^3 + 0 * 2^2 + 0 * 2 + 0 * 20 = 0 + 0 + 128 + 0 + 0 + 0 + 0 + 0 + 0 + 0 = 128$$

$$0100000101 = = 0 * 2^9 + 1 * 2^8 + 0 * 2^7 + 0 * 2^6 + 0 * 2^5 + 0 * 2^4 + 0 * 2^3 + 1 * 2^2 + 0 * 2 + 1 * 20 = 0 + 256 + 0 + 0 + 0 + 0 + 0 + 4 + 0 + 1 = 261,$$

$$0000101100 = = 0 * 2^9 + 0 * 2^8 + 0 * 2^7 + 0 * 2^6 + 1 * 2^5 + 0 * 2^4 + 1 * 2^3 + 1 * 2^2 + 0 * 2 + 0 * 20 = 0 + 0 + 0 + 0 + 32 + 0 + 8 + 4 + 0 + 0 = 44$$

Біз ұсынылған хабарламаны В жиынын және бұрын ұсынылған шифрлау сұлбасын пайдаланып шифрлаймыз, біз аламыз:

$$f(609) = 1 * 43 + 0 * 129 + 0 * 215 + 1 * 473 + 1 * 903 + 0 * 302 + 0 * 561 + 0 * 1165 + 0 * 697 + 1 * 1523 = 43 + 473 + 903 + 1523 = 2942.$$

$$f(686) = 1 * 43 + 0 * 129 + 1 * 215 + 0 * 473 + 1 * 903 + 0 * 302 + 1 * 561 + 1 * 1165 + 1 * 697 + 0 * 1523 = 43 + 215 + 903 + 561 + 1165 + 697 = 3584,$$

$$f(32) = 0 * 43 + 0 * 129 + 0 * 215 + 0 * 473 + 1 * 903 + 0 * 302 + 0 * 561 + 0 * 1165 + 0 * 697 + 0 * 1523 = 903,$$

$$f(46) = 0 * 43 + 0 * 129 + 0 * 215 + 0 * 473 + 1 * 903 + 0 * 302 + 1 * 561 + 1 * 1165 + 1 * 697 + 0 * 1523 = 903 + 561 + 1165 + 697 = 3326,$$

$$f(128) = 0*43 + 0*129 + 1*215 + 0*473 + 0*903 + 0*302 + 0*561 + 0*1165 + 0*697 + 0*1523 = 215,$$

$$f(261) = 0*43 + 1*129 + 0*215 + 0*473 + 0*903 + 0*302 + 0*561 + 1*1165 + 0*697 + 1*1523 = 129 + 1165 + 1523 = 2817,$$

$$f(44) = 0*43 + 0*129 + 0*215 + 0*473 + 1*903 + 0*302 + 1*561 + 1*1165 + 0*697 + 0*1523 = 903 + 561 + 1165 = 2629.$$

Сонымен, ұсынылған хабарлама «*Добро ори клон»* келесі *C* жиынтығына шифрланған

$$C = (2942, 3584, 903, 3326, 215, 2817, 2629).$$

Схема дешифрования текста
V саны есептеледі

$$V \bmod m \equiv t^{-1}C \bmod m \equiv 37 * \mathrm{C} \bmod m \equiv$$
$$\equiv (37 \bullet 2942, 37 \bullet 3584, 37 \bullet 903, 37 \bullet 3326, 37 \bullet 215, 37 \bullet 2817, 37 \bullet 2629) \bmod m,$$

мұндағы *m*=1590.

Есептеулер жүргізейік. Біз келесі мәндерді аламыз:

$$37 * 2942 = 108854 = (68 * 1590 + 734) \bmod 1590 = 734,$$
$$37 * 3584 = 132608 = (83 * 1590 + 638) \bmod 1590 = 638,$$
$$37 * 903 = 33411 = (21 * 1590 + 21) \bmod 1590 = 21,$$
$$37 * 3326 = 123062 = (77 * 1590 + 632) \bmod 1590 = 632,$$
$$37 * 215 = 7955 = (5 * 1590 + 5) \bmod 1590 = 5,$$
$$37 * 2817 = 104229 = (65 * 1590 + 879) \bmod 1590 = 879,$$
$$37 * 2629 = 97273 = (61 * 1590 + 283) \bmod 1590 = 283.$$

Есептеулер нәтижесінде жиынтықты алдық

$$V = (734, 638, 21, 632, 5, 879, 283).$$

Осы жиынтықтың әрбір элементі үшін біз сөмке мәселесін тез өсетін реттілікпен шешеміз

$$A = (1, 3, 5, 11, 21, 44, 87, 175, 349, 701).$$

734 саны үшін біз аламыз: 701 қосыңыз, себебі 701<734. Реттік индекс компоненттер i,

$$i = 1.$$

Біз 734–701 = 33 айырмашылығын табамыз; біз 21–ді қосамыз, өйткені 21<33). Реттік индекс компоненттер *i*,

$$i = 6;$$

біз 33–21 = 12 айырмашылығын табамыз; біз 11–ді қосамыз, өйткені 11<12. Реттік индекс компоненттер *i*,

$$i = 7;$$

біз 12–11=1 айырмашылығын табамыз; 1 қосыңыз. Реттік индекс компоненттер *i*,

$$i = 10;$$

біз 1–1 = 0 айырмашылығын табамыз; 734 шифрының екілік коды келесідей

1001100001.

638 саны үшін біз аламыз: 349 қосыңыз, себебі 349 < 638. Реттік индекс компоненттер *i*,

$$i = 2;$$

біз 638–349 = 289 айырмашылығын табамыз; біз 175 қосамыз, өйткені 175 < 289. Реттік индекс компоненттер *i*,

$$i = 3;$$

біз айырмашылықты табамыз 289–175= 114; 87 қосыңыз, өйткені 87 < 114. Реттік индекс компоненттер *i*,

$$i = 4;$$

біз 114–87 = 27 айырмашылығын табамыз; біз 21 санын қосамыз, өйткені 21 < 27. Реттік индекс компоненттер *i*,

$$i = 6;$$

біз 27–21= 6 айырмашылығын табамыз; 5 < 6 болғандықтан 5 қосамыз. *i* = 8 компоненттерінің реттік индексі; 6–5= 1 айырмашылығын табыңыз; 1 қосыңыз. Реттік индекс компоненттер *i*,

$$i = 10;$$

біз 1–1 = 0 айырмашылығын табамыз; 638 шифрының екілік коды 1010101110 түрінде болады.

21 Саны үшін біз аламыз: 21 қосамыз, себебі 21=21. Реттік индекс компоненттер $i, i = 6$; біз айырмашылықты табамыз 21–21=0; 21 шифрының екілік коды 0000100000 түрінде болады.

632 саны үшін біз аламыз: 349 қосыңыз, себебі 349 < 632. Реттік индекс компоненттер *i*,

$$i = 2;$$

біз 632–349 = 283 айырмашылығын табамыз; біз 175 қосамыз, өйткені 175 < 283. Реттік индекс компоненттер *i*,

$$i = 3;$$

біз айырмашылықты табамыз 283–175= 108; 87 қосыңыз, өйткені 87 < 105). Реттік индекс компоненттер *i*,

$$i = 4;$$

біз 108–87 = 21 айырмашылығын табамыз; біз 21–ді қосамыз, өйткені 21=21). Реттік индекс компоненттер *i*,

$i = 6$;

біз 21–21 = 0 айырмашылығын табамыз; 632 шифрының екілік коды 0000101110 түрінде болады

5 Саны үшін: 5 санын қосыңыз (5 = 5) (i = 8 компоненттерінің реттік индексі); 5–5=0 айырмашылығын табыңыз; 21 шифрының екілік коды келесі түрге ие 0010000000.

879 саны үшін: 701 қосыңыз (701 < 879 дейін) (реттік индекс компоненттер i = 1); айырмашылықты табыңыз 879–701= 178; 175 қосыңыз (175 < 178 дейін); (реттік индекс компоненттер i = 3); айырмашылықты табыңыз 178–175= 3;

3 санын қосыңыз; (реттік индекс компоненттері I = 9); Біз 3–3= 0 айырмашылығын табамыз; 879 шифрының екілік коды келесі түрге ие 0100000101;

283 саны үшін: біз 175 санын қосамыз (175 < 283) (реттік индекс компоненттері i = 3); біз 283–175= 108 айырмашылығын табамыз; 87–ді қосамыз (87 < 108); (реттік индекс компоненттері $i = 4$); біз 108–87=21 айырмашылығын табамыз; 21 санын қосамыз; (реттік индекс компоненттері $i = 6$); біз 21–21= 0 айырмашылығын табамыз; 283 шифрының екілік коды келесі түрге ие 00000101100;

Шифрды ашу нәтижесінде бастапқы хабарламаның екілік коды алынды.

Ұсынылатын әдебиеттер тізімі

1. Абрамов М., Кренделев П. Криптографические защиты информации. / Абрамов М. – CRYPTO, 2022. – 249 с.

2. Blakley GR, Borosh I. Rivest-Shamir-Adleman public key cryptosystems do not always conceal messages. Computers & Mathematics with Applications. 2020, pp.169-178

3. Бияшев М., Петров П. Криптографическия с открытым ключом. / Бияшев М. – М