2.6, Біржақты тесік функциясы және RSA шифры

Оның әзірлеушілері Рон Ривест, Ади Шамир және Леонард Адлеманның атымен аталған бұл шифр әлі күнге дейін кеңінен қолданылатындардың бірі.

«Шәмір» шифры оқу үшін жабық хабар алмасу мәселесін толық шешетінін байқадық, егер абоненттер ашық байланыс желілерін ғана пайдалана алатын болса. Алайда бұл жағдайда хабар бір абоненттен екінші абонентке үш рет қайта бағытталады, бұл кемшілік болып табылады. Эль-Гамаль шифры деректерді бір беруде бірдей мәселені шешуге мүмкіндік береді, бірақ берілетін шифртексттің көлемі хабар көлемінен екі есе үлкен. RSA жүйесінде мұндай кемшіліктер жоқ. Бір қызығы, ол дискретті логарифмнен өзгеше бір құйрықты функцияға негізделген. Сонымен қатар, мұнда біз тағы бір өнертабыспен кездесеміз қазіргі заманғы криптография – бір жақты функция «саңылау» (қақпақты есік функциясы).

Бұл жүйе сан теориясынан мынадай екі фактіге негізделеді:

1) санды қарапайымдылыққа тексеру міндеті салыстырмалы түрде оңай;

2) n = pq (p және q — премьер сандар) формасының факторингтік сандар проблемасы, егер біз тек n, ал p және q үлкен сандарды білсек өте қиын (бұл факторизация проблемасы деп аталады).

A, B, C абоненттері болсын . Әрбір абонент кездейсоқ екі үлкен премьер-нөмірді таңдайды, P және Q, содан кейін санды есептейді

$$N = P\,Q. \qquad (2.28)$$

(N саны басқа абоненттерге қолжетімді ашық ақпарат болып табылады.) Осыдан кейін абонент $\phi = (P-1)(Q-1)$ санын есептеп, ϕ ϕ өзара премьера < кейбір d санын таңдайды, ал жалпыланған Евклид алгоритмі бойынша осындай санды табады.

$$cd \bmod \phi = 1. \qquad (2.29)$$

2.6, Біржақты тесік функциясы және RSA шифры

T a b l i c a 2.4. RSA қызметіндегі пайдаланушы пернелері

Абонент	Құпия кілт	Жалпыға қолжетімді кілт
A	c_A	d_A, N_A
B	c_B	d_B, N_B
C	c_C	d_C, N_C

Абоненттерге қатысты барлық ақпарат және олардың жалпыға қолжетімді және құпия кілттері Кестеде келтірілген. 2.4.

RSA хаттамасын сипаттайық. Алиса M хабарын Бобқа тапсырғысы келеді деп ойлаймын, ал m хабары M < N B теңсіздігін қанағаттандыратын сан ретінде қарастырылады (содан кейін B индексі тиісті параметрлер Бобқа тиесілі екенін көрсетеді)

1-қадам. Алиса формула арқылы хабарды шифрлау

$$e = m^{dB} \bmod N_B, \quad (2.30)$$

Бобтың ашық параметрлерін пайдаланып, e-ді ашық сызықтың үстінен алға жылжыту.

2-қадам. Шифрланған хабарды алған Боб есептейді

$$m' = e^{cB} \bmod N_B. \quad (2.31)$$

Мақұлдау 2.12. Сипатталған хаттама үшін m' = m, яғни B абоненті A-дан шығыс хабарын алады.

Д о с а а е л л т в о . Хаттаманы жасау туралы

$$m' = m^{k\varphi(N_B)+1} \bmod N_B = m.$$

Теңдік (2.29) кейбір k үшін дегенді білдіреді

$$\phi_B = (P_B - 1)(Q_B - 1) = \varphi(N_B),$$

2.5 өтінішке сәйкес

$$c_B d_B = k\phi_B + 1.$$

мұндағы ф(~) — Эулер функциясы. Осыдан Теорема 2.8 келесі

$$m' = e^{c_B} \bmod N_B = m^{d_B c_B} \bmod N_B.$$

2.13 тұжырымы (RSA протоколының сипаттары).

1) хаттама ақпаратты шифрлап, шифрын дұрыс шифрлайды;

2) барлық хабарларды ұстап, барлық ашық ақпаратты білетін шабуылдаушы үлкен P және Q көмегімен бастапқы хабарды таба алмайды.

Дәлел . Хаттаманың бірінші мүлкі 2.12-өтініштен шығады. Екінші қасиетін дәлелдеу үшін, Шабуылдаушы тек N және d жалпыға ортақ параметрлерді ғана білетінін атап өту керек, с табу үшін ол ф = (P − 1)(Q − 1) мәнін білуі тиіс, ал ол өз кезегінде P мен Q-ді білуі керек. Жалпы айтқанда, ол N факторингі арқылы P және Q таба алады, бірақ бұл қиын міндет (бөлімнің басындағы 2-тармақты қараңыз). Ірі кездейсоқ P және Q таңдау қолайлы уақытта мүмкін болатынын ескеріңіз, себебі 1-тармақ шындыққа жанасады.

Бір жақты функция y = x^d mod N , RSA жүйесінде қолданылған, оңай жасауға мүмкіндік беретін «бос саңылау» деп аталады.кері x = функциясын есептеңізhb ^{d}Vy mod N, егер N жай көбейткіштерге ыдырауы белгілі болса. (Шынымен, есептеу оңай ф = (P − 1)(Q − 1), содан кейін c = d^{-1} mod ф.) Егер P және Q белгісіз болса, онда кері функцияның мәнін есептеу іс жүзінде мүмкін емес және N-ден P және Q табу өте қиын, яғни. P және Q білімі -бұл «саңылау» немесе «құпия өткел»). Мұндай бір жақты функцияларсаңылаулары бар криптографияның басқа бөлімдерінде қолданылады

РҚА схемасы үшін әрбір абоненттің P және Q премьер сандарының өз жұбын таңдауы маңызды, яғни барлық модульдер N_A, N_B , N_C . әр түрлі болуы керек (әйтпесе, бір абонент басқа абонентке арналған шифрланған хабарларды оқи алады). Алайда бұл екінші ашық параметрден талап етілмейді d, D параметрі барлық абоненттер үшін бірдей болуы мүмкін. Көбіне d = 3 таңдау ұсынылады (P және Q тиісті таңдауымен [28]) қараңыз. Содан кейін шифрлау мүмкіндігінше тез орындалады, бар болғаны екі көбейтуде

Мысал 2.17. Айталық, Алиса Бобқа m = 15 хабар жібергісі келеді. Боб келесі параметрлерді таңдауға мүмкіндік берсін:

$$P_B = 3,\ Q_B = 11,\ N_B = 33,\ d_B = 3$$

(3 — ϕ(33) = 20- мен өзара. Жалпылама Евклид алгоритмін пайдаланып CB табайық:

$$c_B = 7$$

(тексеру: 3 · 7 mod 20 = 1). Формуланы пайдаланып m кодын (2.30):

$$e = 15^3 \bmod 33 = 15^2 \cdot 15 \bmod 33 = 27 \cdot 15 \bmod 33 = 9$$

9 нөмірі Алиса Бобқа ашық байланыс арнасы арқылы береді. Тек Боб $c_B = 7$ біледі, сондықтан ол алынған хабарды (2.31) пайдалана отырып декодтайды:

$$m' = 9^7 \bmod 33 = \left(9^2\right)^2 \cdot 9^2 \cdot 9 \bmod 33 = 15^2 \cdot 15 \cdot 9 \bmod 33 = 15.$$

Сөйтіп Боб Алисаның хабарын ашып көрсетті.

Қаралған жүйе үлкен P және Q кезінде ашылмайды, бірақ келесі кемшілігі бар: B абонентінің ашық ақпаратын пайдаланып B хабарламасын береді (N B және d B сандары). Шабуылдаушы B-ға арналған хабарларды оқи алмайды, бірақ шабуылдаушы A атынан B-ға хабар бере алады. Мұны төмендегідей күрделі хаттамаларды пайдалану арқылы болдырмауға болады.

A B-ге m хабарламасын жібергісі келеді. Алдымен A $e = m^{cA} \bmod N_A$ санын есептейді. Шабуылдаушы мұны істей алмайды, себебі c_A құпия. Содан кейін A $f = e^{dB} \bmod N_B$ санын есептеп, f нөмірін B-ге жібереді. B f қабылдайды және $u = f^{cB} \bmod N_B$ және $w = u^{dA} \bmod N_A$ сандарын ретімен есептейді.

Нәтижесінде B абоненті w = m хабарын алады. RSA-ның бастапқы схемасындағыдай, шабуылдаушы берілетін хабарды оқи алмайды, бірақ мұнда, RSA-ға қарағанда, ол A атынан да хабар жібере алмайды (себебі ол құпия c_A-ны білмейді)

Бұл жерде біз жаңа жағдаймен бетпе-бет келіп отырмыз. Б хабардың А-дан келгенін біледі, яғни оны құпия с А шифрлаумен «қол қойды» деген түрі Бул электрондық немесе сандық қолтанба деп аталатын мысал. Ол қазырғы заманғы криптографиялық кенінен қолданылатын өнертабыстарының бірі және жүйелі турде 4-тарауда зерттеледі.