Дәріс 7. Ашық кілтті криптография

Жоспар:

1. Ашық кілтті криптография анықтамасы
2. Диффи-Хеллман хаттамасы
3. RSA криптожүйесі

Ашық кілтті криптография анықтамасы

Ашық кілтті криптография идеясы 1976 жылы Диффи мен Хеллманның «Криптографиядағы жаңа бағыттар» атты еңбегінде жарық көрді. Бұл идея F функциясын құруға негізделген, оның көмегімен x аргументінің мәнін біле отырып, $y = F(x)$ тиімді есептеуге болады.

Сонымен қатар, белгілі y мәні бойынша кері есепті қолайлы уақыт аралығында шешу мүмкін емес, яғни x аргументін анықтау мүмкін емес. Мұндай қасиеттері бар функциялар біржақты деп аталады.

Анықтама 1. $F: X \to Y$ функциясы екі қасиетке ие болса, бір жақты деп аталады:

1) $y = F(x)$ мәнін есептеудің көпмүшелік алгоритмі бар;

2) кері есепті шешудің көпмүшелік алгоритмі жоқ, яғни. x мәнін y арқылы анықтау.

Бір жақты функция үшін кері есепті шешу рұқсат етілген және рұқсат етілмеген шешім үшін бірдей мүмкін емес. Бұл қақтығысты шешу үшін Диффи мен Хеллман бір жақты қақпақ функциясының тұжырымдамасын енгізді.

Анықтама 2. Функция $F_k : X \to Y$, K параметріне тәуелді, егер оның үш қасиеті болса, құпия K бар бір жақты деп аталады:

1) кез келген K параметр үшін $y = F_k(x)$ мәнін есептеудің көпмүшелік алгоритмі бар;

2) белгісіз K кезінде кері есепті шешудің көпмүшелік алгоритмі жоқ, яғни x мәнін y арқылы анықтау;

3) белгілі K кері есепті шешудің көпмүшелік алгоритмі бар, яғни x мәнін y арқылы анықтау.

Құпия бір жақты функция үшін кері есепті шешу рұқсат етілген пайдаланушы үшін мүмкін болады, бірақ рұқсат етілмеген адам үшін мүмкін емес болып қалады. Практикалық криптографияда біржақты рөл атқаратын функцияларды құру кезінде сандар теориясының күрделі есептері қолданылады, мысалы:

1) n санын көбейтіңіз;
2) n санының жай екенін анықтаңыз;
3) n-нен үлкен жай санды табыңыз;
4) $x^2 \equiv amodn$ теңдеуінен x санын табыңыз;
5) $a^x \equiv bmodn$ теңдеуінен x санын табыңыз.

Соңғы уақытта эллиптикалық қисықтар теориясына негізделген ашық кілтті криптографиялық әдістер белсенді дамып келеді. Ашық кілтті криптографияның мәні мынада: криптографиялық жүйеде екі түрлі кілт бар. Хабарламаны екі кілті бар адам ғана шеше алады немесе шифрлай алады. Бұл

тәсіл ашық кілттерді пайдаланудың әртүрлі схемаларын жасауға мүмкіндік береді, мысалы:

1) Екі кілтті иеленетін пайдаланушы бар. Бұл жағдайда шифрлау үшін бір кілт, ал шифрды ашу үшін екінші кілт қолданылады. Бұл тәсіл, мысалы, цифрлық қолтаңба жүйелерінде қолданылады, мұнда жеке кілт қолтаңба жасау үшін, ал ашық кілт оны тексеру үшін қолданылады.

2) Бір уақытта екі кілтті иеленетін пайдаланушылар жоқ. Бұл жағдайда бір пайдаланушы шифрлау үшін ашық кілтті, ал екіншісі шифрды ашу үшін жеке кілтті пайдаланады. Бұл принцип асимметриялық шифрлаудың негізінде жатыр, мысалы, RSA алгоритмінде, онда жіберуші хабарламаны алушының ашық кілтімен шифрлайды, ал алушы оны өзінің жеке кілтімен шифрлайды.

Екі схема да ақпараттың сенімді қорғалуын және пайдаланушының аутентификациясын қамтамасыз ететін заманауи криптографиялық жүйелерде кеңінен қолданылады.

Әзірленген схемаға байланысты әртүрлі криптографиялық процедураларды орындауға болады: аутентификация, электрондық қолтаңба, ортақ кілтті қалыптастыру, сонымен қатар криптографиялық хаттамалар, олар өз кезегінде ақпарат алмасуға және деректерді қорғауға байланысты әртүрлі мәселелерді шешеді.

Жоғарыда ұсынылған ашық кілттер схемалары оларды қолданудың мысалдары ретінде сандық қолтаңба мен аутентификация алгоритмдерін қарастырады. Біз бұл ұғымдарды анықтаймыз.

Аутентификация-аутентификация процедурасы. Ол ақпаратты беру кезінде өзара әрекеттесудің барлық аспектілеріне қолданылуы мүмкін: байланыс сеансы, жіберілген хабарлама, хабар көзі және т. б.

Электрондық цифрлық қолтаңба (ЭЦҚ) — берілген және қол қойылған хабарламадан бас тарту мүмкін невозможстігін қамтамасыз ететін рәсім [19].

Айта кету керек, ашық кілтті криптографияның алғашқы нәтижелерін британдық ғалымдар алған, бірақ олар жарияланбаған.

Диффи-Хэллмана сұлбасы

Диффи-Хеллман хаттамасы көптеген шифрлау жүйелерінің негізі болып табылады, тіпті хабар алмасу жағдайында да қауіпсіз деректер алмасуды қамтамасыз етеді. Бұл ашық байланыс арнасы арқылы ортақ кілтті қалыптастыру хаттамасы екі тарапқа ортақ құпия кілтті келісуге мүмкіндік береді, содан кейін оны хабарламаларды симметриялы шифрлау үшін пайдалануға болады. Бұл жағдайда ашық арнаны ұстап алған шабуылдаушы қатысушылардың жабық параметрлерін білмей-ақ бұл кілтті қалпына келтіре алмайды.

Ашық байланыс арнасы арқылы ортақ кілтті генерациялау протоколы;

1) Екі пайдаланушы (абонент) A және B;

2) A және B пайдаланушыларына белгілі p жай саны берілген;

3) $g, g < p - 1$жалпы саны таңдалды;

4) A және B абоненттері сәйкесінше $a,\ 0 < a < p - 1$ және $b, 0 < b < p - 1$

құпия кілттерін дербес таңдайды;

5) A абоненті B абонентіне $g^a mod p$ хабарламасын жібереді;

6) B абоненті A абонентіне $g^b mod p$ хабарламасын жібереді;

7) A абоненті ортақ кілтті есептейді (4.1)

$$k = [g^b]^a mod p; \tag{4.1}$$

8) B абоненті ортақ кілтті есептейді (4.2)

$$k = [g^a]b \ mod \ p. \tag{4.2}$$

Өзара аутентификация хаттамасы

Деректер көзінің аутентификациясының бірнеше схемалары бар [16]. Олардың біреуін жүзеге асырудың шарттары мен алгоритмін көрсетейік:

1) A және B екі абоненті бар;

2) A және B жазылушыларына белгілі p жай саны және $g, g < p - 1$, саны берілген;

3) A және B абоненттері, тиісінше, E_A және E_bашық шифрлау функцияларын және қасиеттері бар жеке шифрды шешу D_A және D_Bфункцияларын иеленеді (4.3).

$$D_A E_A\ (M) = M, \qquad D_B\ E_B(M) = M. \tag{4.3}$$

Мұнда M – жіберілген хабарлама, теңдік функциялардың қолданылу ретіне тәуелді емес;

4) A және B абоненттері сәйкесінше $a, 0 < a < p - 1$ және b, $0 < b < p - 1$ құпия кілттерін дербес таңдайды;

5) A абоненті B абонентіне хабарлама жібереді

$$g^a mod \ p;$$

6) B абоненті:

– ортақ кілтті есептейді $k = [g^a]^b mod p$;

– D_B жеке функциясын пайдаланып, қолтаңбаны (хабарлама) жасайды

$$D_B(g^a mod p, g^b mod p);$$

– k кілтін пайдаланып, қолтаңбаны шифрлайды

$$E_k(D_B(g^a mod p, g^b mod p)),$$

мұндағы E_k– жалпы шифрлау функциясы;

– A абонентіне хабарлама жібереді $g^b mod p, E_k(D_B(g^a mod p, g^b mod p))$;

7) A абоненті:

– ортақ кілтті есептейді $k = [g^a]^b mod p$;

– D_A жеке функциясын пайдаланып, қолтаңбаны жасайды, яғни D_A хабарламасын жібереді ($g^a mod p$, $g^b mod p$);

– k пернесін пайдаланып, E_k қолтаңбасын шифрлайды $D_A(g^a mod p, g^b mod p)$;

– B абонентіне $E_k(D_A(g^a mod p, g^b mod p))$ хабарламасын жібереді;

– есептеу арқылы B қолтаңбаны тексереді

$E_B(D_k(E_k\left(D_B(g^a mod p, g^b mod p)\right))) = g^a mod p, g^b mod p$, мұндағы D_k жалпы шифрды шешу функциясы.

8) B абоненті A-ның қолтаңбасын есептеу арқылы тексереді (4.4)

$$E_A(D_k(E_k\left(D_A(g^a mod p, g^b mod p)\right))) = g^a mod p, g^b mod p. \quad (4.4)$$

RSA криптожүйесі

RSA алгоритмі бірінші ашық кілтті шифрлау алгоритмі болып табылады. RSA жұптастырылған кілттерді пайдалану арқылы қауіпсіздікті қамтамасыз етеді: шифрлау үшін қолданылатын ашық және шифрды ашу үшін қажет жабық. Алгоритмнің негізгі идеясы-ашық кілтті біле отырып, екі жай санның көбейтіндісі болып табылатын үлкен N санын факторизацияламай, жеке кілтті ақылға қонымды уақыт ішінде есептеу мүмкін емес. Жүйе келесі фактілерге негізделген:

1) $a \equiv b^d \ mod \ n$ санның n есептеу модулі қарапайым тапсырма болып табылады;

2) $a \equiv b^d mod \ n$ есептеу, құрама модуль n, теңдеуден b саны қиын тапсырма;

3) егер p және q жай сандар және $n = pq$ екені белгілі болса, онда n–ді есептеу оңай, бірақ n–нің жай көбейткіштерге жіктелуін табу қиын тапсырма;

4) егер $n = pq$ жай көбейткіштерге ыдырауы белгілі болса, онда теңдеуден b санын есептеу тапсырмасы $a \equiv b^d \ mod \ n$ қолданылады.

RSA криптожүйесінің теориялық негізі сандар теориясынан Эйлер теоремасы болып табылады.

(Эйлер) **теоремасы.** Кез келген натурал және жай сандар үшін n және a келесіге тең

$$a^{\varphi(n)} \equiv 1 \ mod \ n.$$

Мұндағы $\varphi(n)$ – Эйлер функциясы 1-ден n-ге дейінгі натурал сандардың n өзара жай сандар болып табылады.

Сандар теориясынан егер p және q жай сандар және $n = pq$ болса, онда екені белгілі

$$\varphi(n) = (p-1)(q-1).$$

Сонымен қатар, Эйлер теоремасынан шығатыны, егер кейбір e саны болса $\varphi(n)$, содан кейін теңдеумен салыстырыңыз

$$de \equiv 1 \, mod \, \varphi(n)$$

немесе басқаша

$$de = k \, \varphi(n) + 1.$$

d қатысты бірмәнді шешілді. Шешім кеңейтілген Евклид алгоритмі арқылы оңай анықталады.

Демек, келесі анық болса, онда

$$de \equiv 1 \, mod \, \varphi(n),$$

және x – берілген ақпарат, онда теңдік ақиқат болады

$$(x^e)^{\,d} \, mod \, n \equiv (x^{k\varphi(n)+1}) \, mod \, n \equiv$$
$$\equiv (x^{\varphi(n)})^{\,k} \, x \, mod \, n \equiv x.$$

RSA жүйесін шын мәнінде, соңғы теңдік жүйе арқылы тұжырымдауға негіз болады

RSA жүйесінің қалыптасуы:

1) біз екі түрлі p және q жай сандарын таңдаймыз;
2) $n = pq$ және $\varphi(n) = (p-1)(q-1)$ есептейміз;
3) $\varphi(n)$ мәніне e санын таңдаймыз;
4) теңдеуден d санын есептейміз

$$de \equiv 1 \, mod \, \varphi(n);$$

5) e және n ашық кілттерін анықтаймыз;
6) d, p, q және $\varphi(n)$ құпия кілттерін анықтаймыз.

Шифрлау алгоритмі:

1) M–ның хабарламасының мәтіні берілген;
2) C шифрлық мәтіні формула бойынша есептеледі (4.5)

$$C = E_k(M) = M^{\,e} \, mod \, n. \qquad (4.5)$$

Дешифрлау алгоритмі:

1) C шифрлық мәтіні берілген.
2) Хабар мәтіні M (4.6) формула бойынша есептеледі

$$M = D_k(C) = C^d mod \, n = (M^e)^{\,d} \, mod \, n = M. \qquad (4.6)$$

Сандық қолтаңба келесідей орындалады:

1) A абоненті және M қолтаңбасының мәтіні бар;

2) RSA жүйесінің құпия кілттері анықталады, атап айтқанда $d, p, q, \varphi(n)$;

3) e және n ашық кілттері анықталған;

4) құпия кілт есептеледі

$$C = M^d \ mod \ n.$$

C хабарламасы A абонентінің қолтаңбасы ретінде қарастырылады, себебі құпия кілт d оған ғана белгілі.

Қол қойылған құжатты тексеру (4.7) формула арқылы есептеледі

$$C^{\,e} = (M^d)^{\,e} \ mod \ n = M, \qquad (4.7)$$

e ашық кілтті пайдалану.

Түсініктеме. Егер A және B абоненттерінде сәйкесінше n_A және n_B, эксклюзивті модульдері бар RSA жүйесі болса, қолтаңба схемасы күрделене түседі. Егер A абоненті қол қойылған хабарламасын алғысы келсе

$$C = M^d \ mod \ n_A$$

B абонентінің ашық кілтімен шифрлау, яғни есептеу

$$C_1 = C^{e\beta} \ mod \ n_B,$$

осылайша M тек B абонентіне қол жетімді, содан кейін мән

$$C_1^{d_B} \ mod \ n_B$$

әрқашан хабарға тең бола бермейді

$$C = M^{\,d} \ mod \ n_A.$$

Ол үшін $n_A < n_B$ теңсіздігінің орындалуы қажет. Ақпаратты берудің осы режимінде пайда болатын соқтығысуды шешу үшін пайдаланушылар кейбір T шегі туралы келіссөздер жүргізіп, екі параметрлер жиынтығын құруы керек: біреуі кіші T модулімен, екіншісі үлкен T модулімен, бұл жағдайда жіберуші өзінің кіші модулін қол қою үшін, ал үлкен алушының модулін шифрлау үшін пайдаланады.

Мысал. RSA аббревиатурасын шифрлаймыз. p=17 және q=31 болсын. Сонда $n = pq = 527$ және келесі мән орындалады

$$\varphi(n) = (p-1)(q-1) = 480.$$

$\varphi(n)$ санына тең болатын e=7 санын таңдайық. Теңдеуді шешу

$$de \equiv 1 \, mod \, \varphi(n)$$

d–ге қатысты Евклид алгоритмі арқылы d=343 санын табамыз. Өйткені

$$-137 = 343 \, mod \, 480,$$

онда d = 343 теңдігі орындалады.

Тексеру:

$$7 \cdot 343 = 2401 * 1 \, mod \, 480.$$

RSA хабарламасын [0, 526] интервалында қамтылған сандар тізбегі ретінде елестетейік. Ол үшін R, S және A әріптерін бес өлшемді екілік векторлар ретінде кодтаймыз, олардың сериялық нөмірлерінің ағылшын алфавитіндегі екілік белгісін пайдаланамыз.

$$R = 18 = (10010), S = 19 = (10011),$$
$$\mathrm{A} = 1 = (00001).$$

Содан кейін $RSA = (100101001100001)$.

Көрсетілген [0, 526] аралығына сәйкестендіріп, келесі код көрінісін аламыз

$$RSA = (100101001), (100001) = (\mathrm{M}_1 = 297, \mathrm{M}_2 = 33).$$

Әрі қарай, біз M_1 және M_2 ретімен шифрлаймыз

$$\mathrm{C1} = \mathrm{E}_{k_1}(M_1) = M_1^e \equiv 297^7 \, mod \, 527 = 474.$$

Бұл ретте біз осы жағдайды пайдаландық

$$297^7 = ((297^2)^3 \, 297) \, mod \, 527 =$$
$$= (200^3 \, (\, mod \, 527\,) \, 297\,) \, mod \, 527,$$
$$C_2 = E_k(M_2) = M^e{}_2 \equiv 33^7 \, mod \, 527 = 407.$$

Нәтижесінде y_1 = 474 және y_2 = 407 шифрленген мәтінді аламыз.

Шифрды шешу кезінде келесі әрекеттер тізбегін орындау керек. Біріншіден, есептеңіз $D_k \, (C_1)^{343} = (C_1)^{343} \, mod \, 527$.

Қуатты көтеру кезінде бұл фактіні пайдалану ыңғайлы екенін ескеріңіз

$$343 = 256 + 64 + 16 + 4 + 2 + 1.$$

Осы ұсыну негізінде біз аламыз

$$474^2 \equiv 174\ mod\ 527, \qquad 474^4 mod\ 527 \equiv 237,$$
$$474^8 mod\ 527 \equiv 307, \qquad 474^{16}\ mod\ 527 \equiv 443,$$
$$474^{32}\ mod\ 527 \equiv 205, \qquad 474^{64}\ mod\ 527 \equiv 392,$$
$$474^{128} mod\ 527) \equiv 307, \qquad 474^{256}\ mod\ 527 \equiv 443,$$

соның арқасында орын алады

$$474^{343}(mod\ 527) \equiv$$
$$\equiv (443 \cdot 392 \cdot 443 \cdot 237 \cdot 174 \cdot 474) mod\ 527 \equiv 297.$$

сияқты

$$474^{343}\ mod\ 527 \equiv 33.$$

Әріптік жазбаға оралсақ, шифрды шешкеннен кейін біз RSA жүйесінде бастапқы хабарламаны аламыз.

Біз RSA жүйесінің беріктігі туралы мәселені талдаймыз. RSA-да құпия кілтті табудың қиындығы n санын жай көбейткіштерге факторизациялаудың күрделілігімен анықталатынын көрсетуге болады. Осыған байланысты p және q сандары n ыдырауы есептеу қиын болатындай етіп таңдалуы керек. Ол үшін келесі талаптарды орындау ұсынылады:

1) p және q сандары жеткілікті үлкен, бір–бірінен тым ерекшеленбеуі және сонымен бірге бір–біріне тым жақын болмауы керек;

2) p және q сандары $(p-1)$ және $(q-1)$ сандарының ең үлкен ортақ бөлгіші аз болатындай болуы керек; ең үлкен ортақ бөлгіш $(p-1, q-1) = 2$ түрінде болғаны жөн;

3) p және q үлкен жай сандар болуы керек;

Анықтама. Егер келесі шарттар орындалса, p жай саны қатты *жай сандар* деп аталады:

$$p \equiv 1\ mod\ r,$$
$$p \equiv s-1\ mod\ s,$$
$$r \equiv 1\ mod\ t,$$

мұндағы p, r, s, t – үлкен жай сандар.

Көрсетілген шарттардың кем дегенде біреуі орындалмаған жағдайда, ыдыраудың тиімді алгоритмдері бар N жай көбейткіштерге бөлінеді.

Қазіргі уақытта түрдің ең үлкен сандары $n = p * q$, белгілі әдістерді қолдана отырып көбейе алады, шамамен 140 ондық бөлшектен тұрады. Сондықтан, ұсыныстарға сәйкес, RSA жүйесіндегі p және q сандарында кемінде 100 ондық бөлшек болуы керек.

Желінің әрбір қатысушысы үшін RSA (n) модулін Мұқият таңдаудың маңыздылығын атап өткен жөн. Осыған байланысты мыналарды атап өтуге болады. Оқырман r, q немесе $\varphi(n)$ үш шамасының бірін біле отырып, RSA

құпия кілтін оңай есептеуге болатындығын өздігінен тексере алады. Сонымен қатар, егер декодтаудың құпия көрсеткіші белгілі болса d, модульдің ыдырауы мүмкін n факторизацияның ықтималдық алгоритмін құруға мүмкіндік беретін факторларға n.

Бұдан шығатыны, шифрлау үшін RSA жүйесін пайдаланатын желінің әрбір қатысушысында криптографиялық төзімділіктің жеткілікті деңгейін қамтамасыз ететін өзінің бірегей p модулі болуы керек.

Шынында да, егер желіде барлығы үшін бірыңғай n модулі қолданылса, онда мұндай байланыс ұйымы негізгі RSA жүйесі тұрақты болуы мүмкін болғанына қарамастан құпиялылықты қамтамасыз етпейді. Басқаша айтқанда, олар жалпы модульмен хаттаманың сәтсіздігі туралы айтады. Дәрменсіздік ерікті экспоненттер жұбын (e_i, d_i) білу, атап өткендей, ыдырауға мүмкіндік беретіндігінен туындайды N көбейткіштерге. Сондықтан, осы желінің кез-келген корреспонденті кез-келген басқа корреспонденттің құпия кілтін таба алады. Сонымен қатар, оны ыдыратпай-ақ жасауға болады n көбейткіштерге (мысалы, [20] қараңыз).

Жоғарыда көрсетілгендей, ашық кілтті шифрлау жүйелері салыстырмалы түрде баяу жұмыс істейді. RSA шифрлау жылдамдығын арттыру үшін іс жүзінде шағын е шифрлау көрсеткіші қолданылады.

Қолданылған 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.Пресс, 2021. – 219 с.