2. Бірінші жалпыға қолжетімді кілт жүйесі - Diffie-Hellman жүйесі

Уитфилд Диффи мен Мартин Хелл-ман криптографияда және оның практикалық қосымшаларында нағыз төңкеріске алып келді. Бұл қорғалған арналар арқылы берілетін құпия кілттерді пайдаланбай ақпаратты қорғауға мүмкіндік берген алғашқы жүйе. Осындай жүйелерді қолдану схемаларының бірін көрсету мақсатында N пайдаланушылармен байланыс желісін қарастырайық, мұндағы N - үлкен сан. Олардың әр жұбы үшін құпия байланыс ұйымдастырғымыз келеді. Егер жеке кілттерді таратудың әдеттегі жүйесін қолданатын болсақ, онда абоненттердің әрбір жұбы өзінің құпия кілтімен қамтамасыз етілуі тиіс, яғни барлық кілттер талап етіледі.$\frac{\boldsymbol{N(N-1)}}{\boldsymbol{2}} = \frac{\boldsymbol{N_2}}{\boldsymbol{2}}$

Егер 100 абонент болса, онда 5000 кілт қажет, бірақ 10^4 абонент болса, онда кілттер $5 \cdot 10$ 7 болуы тиіс, Абоненттер саны көп болса, оларды жеке кілттермен қамтамасыз ету жүйесі өте ауыр әрі қымбатқа түседі.

A, B, C абоненттері үшін байланыс жүйесін құруға рұқсат етілсін. Әрбір абоненттің өзінің құпия және ашық мәліметтері болады. Осы жүйені ұйымдастыру үшін, Үлкен prime нөмірі p және белгілі бір сан g, $1 < g < p - 1$ таңдалады, осылайша жиындағы барлық сандар {1, 2, $\cdot \cdot \cdot \cdot 1 -$ ص} әр түрлі державалар g mod p ретінде ұсынылуы мүмкін (мұндай сандарды табу үшін әр түрлі тәсілдер g, олардың біреуі төменде ұсынылады). p және g сандары барлық абоненттерге белгілі.

Абоненттер құпия сақталатын X_A, X_B, X_C үлкен сандарын таңдайды (әдетте бұл таңдауды кездейсоқ сан датчиктерін пайдалана отырып жасау ұсынылады). Әрбір абонент басқа абоненттерге ашық берілетін Y тиісті нөмірін есептейді.

$$\begin{cases} Y^A = g^{XA} mod p \\ Y^B = g^{XB} mod p \\ Y^C = g^{XC} mod p \end{cases} (2.9)$$

Нәтижесінде келесі кестені аламыз.

2.2-кесте. Diffie-Hellman жүйесіндегі пайдаланушы пернелері

Абонент	Құпия кілт	Жалпыға қолжетімді кілт
A	X_A	Y_A
B	X_B	Y_B
C	X_C	Y_C

Айталық, А абоненті В-мен байланыс сеансын ұйымдастыруға шешім қабылдады, ал екі абонент те Кестеден ашық ақпаратқа қол жеткізе алатын. 2.2, А абоненті Б-ға ашық арна арқылы оған хабарлама бергісі келетіні туралы хабарлайды. А абоненті мәнді есептейді

$$Z_{AB} = (Y_B)^{XA} \, mod p \qquad (2.10)$$

(А-ден басқа ешкім мұны жасай алмайды, себебі X_A саны құпия). Өз кезегінде В абоненті нөмірді есептейді

$$Z_{BA} = (Y_A)^{XB} mod p. \qquad (2.11)$$

2.2. Мәлімдеме 2.2. $Z_{AB} = Z_{BA}$.

Дәлелдеу. Шынымен де

$Z_{AB} = (Y_B)^{XA} \, mod \, p = (g^{XB})^{XA} \, mod \, p = g^{XAXB} \, modp = (Y_A) \, XB \, mod \, p = Z_{BA}.$

2-тарау. Жалпыға қолжетімді криптосжүйелер

(Мұнда бірінші теңдік (2.10), екінші және төртінші (2.9), соңғысынан (2.11) кейін жүреді.

Жүйенің негізгі қасиеттерін атап өтейік:

1) А және В абоненттері ашық байланыс желісі арқылы берілмеген

$Z = Z_{AB} = Z_{BA}$ бірдей санды алды;

2) Ева X_A, X_B құпия сандарын білмейді, сондықтан ол Z_{AB} санын есептей алмайды (жалпы айтқанда, ол Y_A-дан X_A құпия нөмірін табуға тырысуы мүмкін (қараңыз (2.9)), алайда үлкен p кезінде бұл іс жүзінде мүмкін емес (ол миллиондаған жылдарды қажет етеді)).

A және B абоненттері деректерді шифрлау және шифрлау үшін Z_{AB} құпия кілт ретінде пайдалана алады. Сол сияқты абоненттердің кез келген жұбы өздеріне ғана белгілі құпия кілтті есептей алады.

Қазір g санын таңдаудың жоғарыда аталған проблемасына тоқталып кетейік. P өз еркімен берілгенін ескерсек, бұл p − 1 санын факторизациялауға байланысты қиын міндет болуы мүмкін. Мәселе мынада, қарастырылып отырған жүйенің жоғары тұрақтылығын қамтамасыз ету үшін p−1 саны міндетті түрде үлкен премьер-факторды қамтуы тиіс (әйтпесе, полиг-Хеллман алгоритмі, мысалы[28],дискретті логарифмді тез есептейді). Сондықтан көбінесе келесі тәсілді қолдану ұсынылады. p премьер-нөмірі теңдік болатындай етіп таңдап алынады

$$p = 2q + 1,$$

мұндағы q — сондай-ақ премьер-сан. Содан кейін g ретінде теңсіздіктер жарамды кез келген санды алуға болады

$$1 < g < p - 1 \text{ и } g^q \bmod p \neq 1.$$

Мысал 2.2.

P = 23 = 2 · 11 + 1 (q = 11). G параметрін таңдаңыз. G = 3 алуға тырысып көрейік. Тексерейік: $3^{11} \bmod 23 = 1$, сондықтан бұл g жарамсыз. g = 5 алыңыз.

Тексерейік: $5^{11} \bmod 23 = 22$. Осылайша, біз p = 23, g = 5 параметрлерін таңдадық. Енді әрбір абонент құпия нөмірді таңдап, тиісті ашық санды есептейді. X A = 7 таңдалсын, XB = 13. Есептеу

2.3. Сандар теориясының элементтері

$Y_A = 5^7$ мод 23 = 17, $Y_B = 5^{13}$ мод 23 = 21. A және B ортақ құпия құруды шешсін. Ол үшін A есептейді

$Z_{AB} = 21^{7} \bmod 23 = 10$ және B $Z_{BA} = 17^{13} \bmod 23 = 10$ есептейді.

Енді оларда байланыс арнасы арқылы берілмеген ортақ кілт 10 бар.