2.4 Шамир шифрлары

Әди Шамир ұсынған бұл шифр бірінші болып қандай да бір қауісіз арналары мен құпия кіліттері жоқ және бір-бірін ешқашан көрмеген тұлғалар үшін ашық байланыс желісі арқылы құпия хабарлармен алмасуға мүмкіндік берді. (Естеріңізге сала кетейік, Диффи-Хеллман жүйесі тек құпия сөзді құруға мүмкіндік береді, ал хабарламаны жіберу үшін бұл сөз кілт ретінде қолданылатын кейбір шифрды қолдану қажет болады.)

Жүйенің сипаттамасына көшейік. Байланыс желісімен байланысқан екі A және B абоненттері бар деп ойлаймыз. M хабарын B абонентіне оның мазмұнын ешкім білмейтіндей етіп бергісі келеді. Кездейсоқ үлкен p нөмірін таңдайды және оны B. A-ға ашық береді, содан кейін екі санды C_A және d_A таңдайды .

$$C_A d_A \text{ мод } (p - 1) = 1.$$

A бұл сандарды құпия сақтайды және бермейді. B сондай-ақ екі cB және dB сандарын таңдайды, сол сияқты

$$c_B d_B \text{ мод } (p - 1) = 1$$

және оларды құпия сақтайды. Содан кейін үш сатылы хаттаманы пайдаланып өз хабарын m-ге береді. Егер $m < p$ (м сан ретінде қарастырылса), онда m хабарламасы дереу беріледі, егер $m \geq p$ болса, онда хабарлама m_1, m2 , …. , m_t мұндағы барлық $mi < p$ түрінде беріледі, содан кейін біріздділікпен m_1, m2 , …. , m_t . Бұл ретте әрбір ми кодтау үшін жаңа жұптарды (c_A, d_A) және (c_B, d_B) кездейсоқ таңдаған дұрыс- әйтпесе жүйенің сенімділігі төмендейді. Қазіргі кезде мұндай шифр, әдетте, сандарды беру үшін қолданылады, мысалы, мәндері p.-дан аз құпия кілттер. Осылайша, біз тек $m < p$. жағдайын ғана қарастырамыз, Хаттаманың сипаттамасын береміз.

1-қадам. Санды есептейді

$$x_1 = m^{c\ A} \bmod p \qquad (2.19)$$

мұндағы m — бастапқы хабар, ал x1-ден B-ға дейін қайта бағыттайды.

2-қадам. B, x_1 алғаннан кейін санды есептейді

$$x_2 = x\ {}_1^{c\ B} \bmod p \qquad (2.20)$$

және x_2-ден A-ға өтеді.

3-қадам. Санды есептейді

$$x_3 = x_2^{\ dA} \ \bmod p \qquad (2.21)$$

және оны B-ға тапсырады

4-қадам. B, x3 алу , санды есептейді

$$x_4 = x_3^{\ dB} \ \bmod p \qquad (2.22)$$

Шамир хаттамасының қасиеттері.

1) $x_4 = m$, яғни хаттаманы іске асыру нәтижесінде бастапқы хабар іс жүзінде A-дан B-ға беріледі;

2) шабуылдаушы қай хабардың берілгенін біле алмайды.

Дәлел . Біріншіден, кез келген бүтін сан $e \geq 0$ $e = k(p - 1) + r$, мұндағы $= e \bmod (p - 1)$ ретінде ұсынылуы мүмкін. Сондықтан Ферматеоремасы негізінде

$x^e \bmod p = x^{k(p-1)+r} \bmod p = (1^k \cdot x^r\ ) \bmod p = x^{\ e \bmod (p-1})) \bmod p.$

Мәлімдеменің бірінші нүктесінің негізділігі мынадай теңдік тізбегінен шығады:

$$x_4 = x_3^{\ dB} \ \bmod p = (x_2^{dA}\ )^{\ dB} \bmod p = (x_1^{cB})^{dAdB} \bmod p =$$

$$= (m^{ca})^{cBdAdB} \bmod p =$$

$$= m^{cAdAcBdB} \bmod p = m^{(cAdAcBdB \bmod (p-1)} \bmod p = m$$

Өтініштің екінші нүктесінің дәлелі м анықтауға тырысатын шабуылдаушы үшін төмендегіден де тиімді стратегия жоқ деген жорамалға негізделеді. Алдымен ол C_B-ді (2.20) есептейді, содан кейін d_B табады да, ақырында $x_4 = m$ from (2,22) деп есептейді. Бірақ бұл стратегияны жүзеге асыру үшін шабуылдаушы дискретті логарифм мәселесін (2.20) шешуі тиіс, бұл іс жүзінде үлкен p-мен мүмкін емес.