2.5. Эль-Гамаль Шифры.

A, B, C, абоненттері болсын . . . бергісі келетіндер

бір-біріне қауіпсіз байланыс арналары жоқ шифрланған хабарламалар. Бұл бөлімде біз осы мәселені шешетін Эль-Гамаль (Taher ElGamal) ұсынған шифрды қарастырамыз,

Шамир шифрынан айырмашылығы, тек бір хабарлама жіберуді қолдану. Шын мәнінде, мұнда Диффи-Хеллман схемасы қолданылады,

екі абонент үшін ортақ құпия кілтті қалыптастыру,

бір-біріне хабарлама жібереді, содан кейін хабарлама шифрланады

оны осы кілтке көбейту арқылы. Әрбір келесі хабарлама үшін құпия кілт қайта есептеледі. Дәлдікке көшейік

әдістің сипаттамасы.

Абоненттердің бүкіл тобы үшін кейбір үлкен жай P және G саны таңдалады, мысалы, әртүрлі G дәрежелері p модулі бойынша әртүрлі сандардың мәні болып табылады (бөлімді қараңыз. 2.2). P және g сандары беріледі

абоненттер ашық түрде (оларды желінің барлық абоненттері қолдана алады).

Содан кейін топтың әр абоненті өзінің құпия нөмірін таңдайды

ci, 1 < ci < p−1 және оған сәйкес келетін ашық di санын есептейді,

$d_i = g^{Ci} \bmod p$. (2.24)

Нәтижесінде біз 2.3 кестесін аламыз.

Кесте 2.3. Жүйедегі пайдаланушы кілттері

Эль-Гамала

Абонент	Секретный ключ	Открытый ключ
A	c_A	d_A
B	c_B	d_B
C	c_C	d_C

Енді А М хабарламасын В абонентіне қалай жіберетінін көрсетейік, Шамир шифрын сипаттау сияқты, хабарлама m < p саны түрінде ұсынылған деп болжаймыз.

1-қадам. А кездейсоқ k санын құрайды, 1 ≤ k ≤ p-2, есептейді

Сандар

$$r = g^k \bmod p, \qquad (2.25)$$

$$e = m \cdot {d_B}^k \bmod p \qquad (2.26)$$

және сандар жұбын (r ,e) В абонентіне береді

2-қадам. В (r ,e) алу арқылы есептейді

$$m' = e \cdot r^{p-1-c_B} \bmod p. \qquad (2.27)$$

Бекіту 2.11(Эль-Гамаль шифрының қасиеттері).

1) В абоненті хабарлама алды, яғни m0 = m;

2) қарсылас p, g , dB , r және e-ді біле отырып, m есептей алмайды.

Дәлел . (2.27) мәнін (2.26)е мәніне ауыстырайық:

$$m' = m \cdot {d_B}^k \cdot r^{p-1-c_B} \bmod p.$$

Енді r орнына (2.25), ал d_b орнына - (2.24):

$$m' = m \cdot (g^{c_B})^k \cdot (g^k)^{p-1-c_B} \bmod p =$$
$$= m \cdot g^{c_B k + k(p-1) - k c_B} \bmod p = m \cdot g^{k(p-1)} \bmod p.$$

Ферма теоремасы бойынша;

$$g^{k(p-1)} mod\ p = 1^k mod\ p = 1,$$

осылайша біз мәлімдеменің бірінші бөлігін аламыз.

Екінші бөлімді дәлелдеу үшін қарсыластың жоқ екенін ескеріңіз

есептей алады к теңдікте (2.25), өйткені бұл дискретті логарифмдеу мәселесі. Сондықтан ол m есептей алмайды

теңдікте (2.26), өйткені M оған белгісіз болып көбейтілді

саны. Қарсылас сонымен қатар хабарламаның заңды алушысының (B абонентінің) әрекеттерін қайталай алмайды, өйткені ол білмейді

cb құпия саны (cb негізінде есептеу (2.24) — сондай-ақ

дискретті логарифмдеу мәселесі).

Мысал 2.16. Біз m = 15 хабарламасын A-дан B-ға жібереміз, біз параметрлерді мысалда қалай жасалғанына ұқсас етіп таңдаймыз

2.2 20 бет. P = 23, g = 5 алайық. Абонент B үшін таңдасын

өзі Құпия Сан cB = 13 және есептелген (2.24)

$$d_b = 5^{13} mod\ 23 = 21$$

A абоненті k = 7 сияқты кездейсоқ k нөмірін таңдайды және (2.25), (2.26)бойынша есептейді:

$$r = 5^7 \bmod 23 = 17, \quad e = 15 \cdot 21^7 \bmod 23 = 15 \cdot 10 \bmod 23 = 12.$$

Енді А В-ге сандар жұбы ретінде шифрланған хабарлама жібереді (17, 12). В есептейді (2.27)

$$m' = 12 \cdot 17^{23-1-13} \bmod 23 = 12 \cdot 17^{9} \bmod 23 = 12 \cdot 7 \bmod 23 = 15.$$

Біз В жіберілген хабарламаның шифрын шеше алғанын көреміз.

Ұқсас схема бойынша барлығы хабарламаларды жібере алатыны анық

желідегі абоненттер. Кез-келген абонент ашық екенін білетінін ескеріңіз

В абонентінің кілті оған шифрланған хабарламалар жібере алады

ашық DB кілтін пайдалану . Бірақ тек В Абоненті және ешкім жоқ

екіншісі, бұл хабарламаларды белгілі арқылы шеше алады

тек оған cB құпия кілті . Сондай-ақ, шифрдың көлемі

хабарлама көлемінен екі есе көп, бірақ тек біреуі қажет

деректерді беру (ашық кілттер кестесі болған жағдайда

барлық абоненттерге алдын-ала белгілі).