Дәріс 8. Асимметриялық криптожүйелер

- Дәріскер: PhD Темирбекова Ж.Е.

Жоспар:

- Эль-Гамаль сұлбасы
- Шнорр сұлбасы
- Цифрлық қолтаңбаны қалыптастыру алгоритмі
- Криптографиялық жүйені қалыптастыру алгоритмі

Эль-Гамаль сұлбасы

Алгоритм кезеңдері:

- p жай санын таңдаймыз;
- біз екі кездейсоқ сандарды таңдаймыз $g, g < p$ және $x, x < p$
- $y=gxmodp$ есептейміз.

Эль–Гамаль схемасының ашық кілті y, g және p сандары, құпия кілті x саны болып табылады.

Сандық қолтаңбаны құру алгоритмі:

- M хабары беріледі, оған қол қою керек;

2) $k, k < p$ кездейсоқ $p-1$ өзара жай санын таңдаймыз;

3) келесіні есептейміз $a=gkmodp$;

4) $M= xa+kbmod\ p-1$ теңдеуден (4.8) формула арқылы b–ні анықтаңыз

5) қолтаңба қалыптастыру. Қолтаңба сандар жұбы (a, b) болып табылады.

k саны құпия кілт болып табылады.

Назар аударыңыз. Төртінші қадамда ЭЦҚ генерациялау кезінде M мәнінің орнына μ=H(M) мәнін пайдалануға болады, мұндағы H – хэш–функция.

Эль-Гамаль схемасындағы цифрлық қолтаңбаны тексеру келесідей:

1) M хабарламасы және (a, b) қолтаңба берілген.

2) есептейміз $yaa\ bmod\ p=gxaab=gxagxb=gxa=xb=gMmodp$;

3) $g^M\ mod\ p$ есептейміз;

Егер мәні келесідей болса $yaa\ bmod\ p$ мәні $gM\ mod\ p$ сәйкес келсе, онда қолтаңба дұрыс.

Шифрды шешу алгоритмі 1:

- M хабарлама берілді;
- $p-1$ өзара жай санымен кездейсоқ $k, k < p$ санын таңдаймыз;
- $a=gkmodp$ есептейміз;
- хабарламаны (4.9) формула арқылы шифрлаймыз

Шнорр сұлбасы

- Шнорр сұлбасын қалыптастыру алгоритмі
- 1) p және q екі жай сандарын таңдаңыз, сонда q көбейткіш болады $(p-1)$;
- 2) a мәнін таңдаңыз, Бұл $a \neq 1$ және $a^q \equiv 1 \, mod \, p$;
- 3) кездейсоқ санды таңдаңыз $s, s < q$.
- 4) $y = a^{-s} \, mod \, p$ есептеңіз.
- Шнорр сұлбасының ашық кілті-p, q және a сандары. Құпия кілт - y саны.
- .

Цифрлық қолтаңбаны қалыптастыру алгоритмі

- Цифрлық қолтаңбаны қалыптастыру алгоритмі келесідей орындалады:
- 1) M хабарламасы және $H(M)$ хэш функциясы берілген;
- 2) кездейсоқ $r, r < q$ санын таңдаңыз;
- 3) $x = a^r \ mod \ p$ есептеңіз;
- 4) M хабарламасына x мәнін қосып, $e = H(M, x) \ mod \ q$ есептеңіз;
- 5) $v = (r + se) \ mod \ q$ мәнін есептеңіз;
- 6) біз қолтаңба жасаймыз. Қолтаңба сандар жұбы (e, v).
- *Назар аударыңыз. r саны-құпия сан.*

- Екі вектордың скаляр көбейтіндісін пайдаланып жаза аламыз.
- $f(x) = A\,x$ мұндағы А және x - n өлшемді векторлар. Енгізілген функцияны пайдалану $f(x) = A\,x$, алдыңғы теңдік $3231 = 129 + 473 + 903 + 561 + 1165$ келесі түрде жазуға болады
-
- $0 * 43 + 1 * 129 + 0 * 215 + 1 * 473 + 1 * 903 + 0 * 302 +$
- $+1 * 561 + 1 * 1165 + 0 * 697 + 0 * 1523 =$
- $= f(0101101100) =$
- $= f(364) = 129 + 473 + 903 + 561 + 1165 = 3231,$
-
- өйткені 0101101100 екілік саны ретінде ұсынылуы мүмкін
-
- $0101101100 = 0 * 10^9 + 1 * 10^8 + 0 * 10^7 + 1 * 10^6 +$
- $+1 * 10^5 + 0 * 10^4 + 1 * 10^3 + 1 * 10^2 + 0 * 10^1 + 0 * 10^0 =$
- $= 0 * 2^9 + 1 * 2^8 + 0 * 2^7 + 1 * 2^6 + 1 * 2^5 + 0 * 2^4 + 1 * 2^3 + 1 * 2^2 + 0 * 2^1 + 0 * 2^0 = 0 + 1 * 256 + 0 + 1 * 64 + 1 * 32 + 0 + 8 + 4 + 0 + 0 = 256 + 64 + 32 + 8 + 4 = 364.$

Криптографиялық жүйені қалыптастыру алгоритмі

- Жылдам өсетін жиынтықты анықтау
- $A = (a_1, a_2, \ldots, a_n)$;
- m модулін келесі теңсіздік орындалатындай етіп таңдаңыз:
- $m > S = a_1 + a_2 + \ldots + a_n$;
- m-ге салыстырмалы жай болатын t бүтін кездейсоқ санды (көбейткіш) таңдаймыз.
- t^{-1} санын t-ге кері есептейміз, яғни келесідей орын алады
- $tt^{-1} \equiv 1 \, mod \, m.$
- $A = (a_1, a_2, \ldots, a_n)$ жиынынан жиынды есептейміз
- $B = (b_1, b_2, \ldots, b_n)$

Мәтінді шифрлау сұлбасы

СИМВОЛ	КОД
Бос орын	00000
Д	10011
О	00001
Б	10101
Р	01110
И	00100
К	01000
Л	00101
Н	01100.

Ұсынылатын 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