1 Криптосистема Эль Гамаля

Рассматриваемая ниже криптосистема Эль Гамаля является системой вероятностного шифрования. Шифр обозначения зависят от случайного выбираемого в каждом сеансе зашифрования параметра.

Алгоритм генерации ключей в этой системе следующий.

Абонент A криптосистемы Эль Гамаля для обеспечения возможности передачи ему секретной информации на открытом ключе выбирает большое простое число p, образующий элемент $\alpha \in Z_p^*$ и секретный ключ $a \in Z_p^* \setminus \{p-1\}$. Как видим, безопасность секретного ключа гарантируется, если в группе Z_p^* проблема дискретного логарифма трудна. Далее он вычисляет степень $y = \alpha^a \bmod p$.

Тройка чисел (p, α, y) есть *открытый ключ шифрования* и публикуются через центр сертификации открытых ключей. Число a составляет секретную *лазейку* и сохраняются как секретный ключ абонента A.[1].

Любой отправитель B, получив от центра сертификации сертификат открытого ключа абонента A, имеет возможность зашифровать секретное сообщение $m,\ 0 < m < n$, и безопасно передать его абоненту A в виде пары чисел (C_1, C_2) из $Z_p^* \times Z_p^*$. (Более длинные сообщения предварительно разбиваются на блоки, последовательно шифруемые и передаваемые абоненту A). Алгоритм E_A зашифрования абонентом B имеющегося сообщения для абонента A рассматривается ниже.

Отсюда, криптосистема Эль-Гамаля $\Sigma_A(X, K, Y, E, D)$ определяется, следующим образом. В этой системе

$$X = Z_p^*,\ Y = Z_p^* \times Z_p^*,\ K = \{(p, \alpha, \beta, a) | \alpha^a \equiv \beta (\bmod\ p)\},$$

где p – достаточно большое простое число, α – образующий элемент группы Z_p^*, a – целое число из интервала $1 \leq a \leq p-2$. Ключ $k = (p, \alpha, \beta, a)$ представляется в виде открытого ключа $k_3 = (p, \alpha, \beta)$ и секретного ключа $k_p = (a)$.

Правило зашифрования на ключе k_3 определяется формулой $E_{k_3}(m) = (C_1, C_2)$, где

$$C_1 \equiv \alpha^r (\bmod\ p),\ C_2 \equiv m \cdot \beta^r (\bmod\ p,)$$

а r – случайно выбираемое число (рандомизатор) из интервала $0 \leq r \leq p-2$.

[1]Абонент A проходит в центре сертификации открытых ключей аутентификацию некриптографического характера, предъявляет открытый ключ и криптографическим методом доказывает, что владеет соответствующим ему секретным ключом. При этом возможно использование протокола доказательства с нулевым разглашением секрета. Центр сертификации публикует открытый ключ данного абонента в составе сертификата открытого ключа за своей цифровой подписью,ключ проверки которой известен всем абонентам компьютерной сети. Использование сертифицированного открытого ключа гарантирует,что зашифрованная на этом ключе информация может быть расшифрована только владельцем соответствующего секретного ключа, имя которого указывается в сертификате открытого ключа

Правило расшифрования на ключе k_p определяется формулой

$$D_{k_p}(C_1, C_2) = C_2 \cdot (C_1^a)^{-1} \text{mod } p.$$

При этом выполняется равенство $D_{k_p}(E_{k_3}(m)) = m$ при любых $k = (k_3, k_p) \in K$ и $m \in X$.

Введение рандомизатора r делает шифр Эль-Гамаля шифром многозначной замены. Это пример схемы *вероятностного шифрования.* Открытый текст и ключ не определяют шифртекст однозначно.

Рандомизатор r должен изменяться при зашифровании различных открытых текстов m и m'. В противном случае соответствующие шифртексты $(C_1,\ C_2)$ и $(C_1',\ C_2')$ будут связаны соотношением $C_2 \cdot (C_2')^{-1} = m \cdot (m')^{-1}$ и m' может быть легко вычислен, если известен m.

Пример 1. Пусть $p = 127, \alpha = 14, a = 51, \beta = \alpha^a \bmod p = 14^{51} \mod 127 = 5$.
Ключевая информация:$K = (p,\ \alpha,\ \beta,\ a) = (127, 14, 5, 51)$;
Открытый ключ: $K_3 = (p,\ \alpha,\ \beta) = (127, 14, 5)$,
Секретный ключ: $K_p = (a) = (51)$.
Пусть m= 100.
Зашифрование: пусть выбран рандомизатор $r = 11$.
$E_{k_3}(100) = (C_1, C_2) = (\beta^r \mod p, m \cdot \beta^r \mod p) = (14^{11} \mod 127, 100 \cdot 5^{11} \mod 127) = (78, 100 \cdot 54 \mod 127) = (78, 66)$.
Расшифрование:
$D_{k_p} = (C_1, C_2) = D_{51}(78, 66) = C_2 \cdot (C_1^a)^{-1} \mod p = 66 \cdot (78^{51})^{-1} \mod 127 = 66 \cdot 54^{-1} \mod 127 = 66 \cdot 40 \mod 127 = 100$.

Пример 2. Пусть $m = 100$ и зашифрование произведено как в примере выше, то есть получен шифртекст $E(100) = (78, 66)$. Пусть в тех же условиях и с использованием того же рандомизатора $r = 11$ зашифровали $m' = 89$: $E_{k_3}(89) = (C_1', C_2') = (\beta^r \bmod p, m \cdot \beta^k \mod p) = (14^{11} \mod 127, 89 \cdot 5^{11} \mod 127) = (78, 89 \cdot 54 \mod 127) = (78, 107)$.
$D_{k_p}(C_1', C_2') = D_{51}(78, 107) = C_2 \cdot (C_1^a)^{-1} \mod p = 107 \cdot (78^{51})^{-1} \mod 127 = 107 \cdot (54)^{-1} \mod 127 = 107 \cdot 40 \mod 127 = 89$. Вычислим m' с использованием $m = 100, C_2 = 66$ и $C_2' = 107$: $m' = m(C_2')(C_2)^{-1} \mod 127 = 100 \cdot 107 \cdot 66^{-1} \mod 127 = 100 \cdot 107 \cdot 102 = 89$.

Данная схема шифрования может быть реализована и при использовании других групп.

Стойкость системы Эль-Гамаля определяется сложностью решения задачи дискретного логарифмирования в Z_p^*.

Можно показать, что при случайном выборе открытого текста эта система обладает полной секретностью относительно атаки по выбираемому открытому тексту тогда и только тогда, когда трудна проблема Диффи-Хеллмана.

Действительно, пусть имеется вероятностный алгоритм, решающий проблему Диффи-Хеллмана, то есть вычисляющий $\alpha^{k_1 k_2}$ по $\alpha, \alpha^{k_1}, \alpha^{k_2}$ в данной группе. Тогда, зная $y = \alpha^a$, $C_1 = \alpha^r$ и $C_2 = m\alpha^{ar}$ вычислим α^{ar}, $m = C_2 \alpha^{-ar}$. С другой стороны, если с некоторой предпочтительной вероятностью найдем m по $C_1 = \alpha^r$, $y = \alpha^a$ и C_2, то сможем решить также проблему Диффи-Хеллмана. Примем $a = k_1,\ r = k_2$. Тогда в качестве открытого ключа имеем (α, α^{k_1}), а в качестве шифртекста –

$$(C_1, C_2) = (\alpha^{k_2}, C_2),$$

где C_2 - произвольно. Применяя алгоритм дешифрования, использующий только α, α^{k_1} и α^{k_2}, получим число m такое, что $\alpha^{k_1 k_2} m = C_2$. Далее получим $\alpha^{k_1 k_2} = C_2 m^{-1}$.

2 Контрольные вопросы

1. Какой трудной проблеме теории чисел соответствует безопасность криптосистемы Эль Гамаля?

2. Какие предосторожности следует соблюдать при выборе параметров криптосистемы Эль Гамаля?

3. Каковы условия полной секретности криптосистемы Эль Гамаля относительно атаки по случайно выбираемому открытому тексту?

4. Почему недопустимо повторное использование рандомизатора?

Литература.

1. Алферов А.А., Зубов А.Ю., Кузьмин А,С., Черемушкин А.В. Основы криптографии. – М: Гелиос АРВ, 2001.