ОБ АНАЛОГЕ СХЕМЫ ЭЛЬ-ГАМАЛЯ НА ОСНОВЕ КВАЗИГРУПП

Малютина Надежда

ПГУ им. Т.Г. Шевченко, Тирасполь, Молдова

231003.bab.nadezhda@mail.ru

1. Введение

Классическая схема Эль-Гамаля представляет собой криптосистему с открытым ключом, работа которой основывается на сложности вычисления дискретных логарифмов и формулируется на языке теории чисел с использованием умножения по модулю простого числа [1].

Перед отправкой сообщения по открытому каналу связи от A к B, первый участник шифрует сообщение, а второй, получив зашифрованное сообщение, расшифровывает его. Предполагается, что используемый для пересылки канал связи доступен для прослушивания третьим лицам. То есть у отправителя и получателя есть противник E, который способен осуществить перехват пересылаемого по этому каналу сообщения. Отправителя принято называть Бобом, получателя – Алисой, а злоумышленника –Евой. Считается, что Ева имеет в своем распоряжении мощное вычислительное оборудование и владеет методами криптоанализа. Алиса и Боб естественно заинтересованы в том, чтобы их сообщения были непонятны Еве, и для этого используют специальные шифры.

Каждая попытка взломать шифр называется атакой на шифр. В криптографии принято считать, что противник может знать используемый алгоритм шифрования, природу передаваемых сообщений и перехваченный зашифрованный текст, но не владея секретным ключом он не в состоянии взломать этот шифротекст.

Основная задача разработчиков современных криптосистем – это создать шифр максимально неуязвимый ко всем известным типам атак на известный или выбранный текст.

2. Схема Эль-Гамаля

Предположим, есть абоненты A и B, которые хотят передавать зашифрованные сообщения друг другу. Рассмотрим схему, предложенную Тахером Эль-Гамалем, которая решает эту проблему, используя только одну пересылку сообщений. Эта схема работает в три этапа: генерации ключей, шифрование и дешифрование.

Этап 1. Генерация ключей.

1) Выбирается случайное просто число p;

2) Выбирается целое число g – первообразный корень p (важным моментом является то, что уже составлены таблицы для минимальных первообразных корней простых чисел, которыми

можно воспользоваться, что позволяет легко преодолеть этот этап, без трудоемких вычислений)**;**

Числа p и g передаются абонентам в открытом виде.

3) Затем каждый абонент выбирает свой секретный ключ c_A и c_B, удовлетворяющие условиям $1 < c_A < p-1, 1 < c_B < p-1$, где числа c_i и $p-1$ взаимно просты;

4) Каждый абонент, используя свой секретный ключ, вычисляет соответствующий открытый ключ:

$$d_A \equiv g^{c_A}(mod\ p) \quad \text{и} \quad d_B \equiv g^{c_B}(mod\ p) \tag{1}$$

Пусть B отправляет сообщение m, представленное как число $m < p$, подписчику A.

Этап 2. Шифрование. B формирует случайное число k – это сессионный ключ, $1 \leq k \leq p-2$, при этом k и $(p-1)$ взаимно просты. Вычисляется пара чисел (r, e) для передачи абоненту A:

$$r \equiv g^k\ (mod\ p) \tag{2}$$

$$e \equiv m \cdot d_B^k\ (mod\ p) \tag{3}$$

Этап 3. Дешифрование. A, получив пару (r, e) и зная закрытый ключ c_A вычисляет:

$$m' \equiv e \cdot r^{p-1-c_A}\ (mod\ p) \tag{4}$$

Абонент A в итоге получит сообщение $m' = m$.

Пример 2.1. Рассмотрим передачу сообщения $m = 506$ от B к A.

Этап 1. Генерация ключей.

1) Возьмем случайное простое число $p = 719$.

2) Выбираем целое число $g = 11$ – наименьший первообразный корень 719**.**

3) Затем абоненты выбирают свои секретные ключи. Пусть абонент B выберет для себя секретное число $c_B = 19$ и абонент A выберет для себя секретное число $c_A = 23$.

4) Каждый абонент вычисляет соответствующий открытый ключ, используя формулу (1):

$$d_A \equiv 11^{23}\ (mod\ 719) = 711,$$

$$d_B \equiv 11^{19}\ (mod\ 719) = 449.$$

Этап 2. Шифрование. Абонент B случайным образом выбирает число $k = 97$ и вычисляет пару чисел (r, e) по формулам (2) и (3) для передачи абоненту A:

$$r \equiv 11^{97}(mod\ 719) = 371,$$

$$e \equiv 506 \cdot 711^{97}(\ mod\ 719) \equiv 506 \cdot 19\ (mod\ 719\ ) = 267.$$

Теперь B отправляет зашифрованное сообщение в виде пары чисел $(371, 267)$.

Этап 3. Дешифрование. A получает пару $(371,267)$ и вычисляет по формуле (4):

$$m' \equiv 267 \cdot\ 371^{719-1-23}\ (mod\ 719) \equiv \quad 267 \cdot\ 371^{695}\ (mod\ 719) \equiv$$

$$\equiv 267 \cdot 492\ (mod\ 719) = 506.$$

Итак, A смог расшифровать переданное сообщение 506.

Противник, зная p, g, d_A, r и e, не может вычислить m. Только A может расшифровать сообщение с помощью своего секретного ключа c_A, известного только ему.

Схему Эль-Гамаля из-за случайности выбора числа k называют схемой вероятностного шифрования или шифром многозначной замены. Вероятностный характер шифрования является её преимуществом. В схеме Эль-Гамаля необходимо использовать различные значения случайной величины k для шифровки различных сообщений. Недостатком схемы является удвоение длины зашифрованного текста по сравнению с первоначальным текстом.

Эту схему можно переформулировать в терминах кольца вычетов по модулю p или, что то же самое, на языке поля Галуа $GF(p)$. Пусть $(Z_p,+)$ $-$ циклическая группа вычетов большого простого порядка относительно сложения вычетов, а a $-$ генератор группы.

$$(Z_{p-1},\cdot) \cong Aut(Z_p,+)(gcd(a, p-1) = 1)$$

Этап 1. Генерация ключей.

Ключи Алисы следующие: Открытый ключ: p, a и $a^m, m \in \mathbb{N}$. Закрытый ключ: m.

Этап 2. Шифрование. Чтобы отправить сообщение $b \in (Z_{(p-1)}, \cdot)$, Боб вычисляет a^r и a^{mr} для случайного $r \in \mathbb{N}$ (иногда число r называется эфемерным ключом [3]).

Зашифрованный текст будет иметь вид : $(a^r;\ a^{mr} \cdot b)$.

Этап 3. Дешифрование. Алиса знает m, поэтому, если она получит зашифрованный текст $(a^r;\ a^{mr} \cdot b)$, она вычислит a^{mr} из a^r, а затем a^{-mr}, а затем из $a^{mr} \cdot b$ вычислит b .

Пример 2.2. Алиса выбирает $p = 719, a = 11, m = 23$ и вычисляет:

$$a^m \equiv 11^{23}(mod\ 719) = 711\ (mod\ 719).$$

Ее открытый ключ: $(p, a^m) = (719,711)$, а ее закрытый ключ: $m = 23$.

Боб хочет отправить Алисе сообщение «S». Он выбирает случайное целое число $r = 19$ и шифрует $S = 506$ как $(a^m)^r \cdot S$. Боб получает:

$$(11^{19}, 11^{437} \cdot 506)(mod\ 719) \equiv (449,510 \cdot 506)(mod\ 719) \equiv (449,658)(mod\ 163).$$

Он отправляет Алисе зашифрованное сообщение $(449,658)$. Алиса получает это сообщение и, используя свой закрытый ключ $m = 23$, расшифровывает его следующим образом:

$(449^{-23} \cdot 658)(mod\ 719) \equiv (449^{695} \cdot 658)(mod\ 719) \equiv (86 \cdot 658)(mod\ 719) = 506.$

Таким образом, различные точки зрения на одну и туже математическую идею могут привести к различным обобщениям и новым модификациям классических алгоритмов.

3. Аналог схемы Эль-Гамаля, основанный на алгоритме Марковского

Приведем аналог системы шифрования Эль-Гамаля на основе алгоритма Марковского [4,5].

Пусть (Q, f) бинарная квазигруппа и $T = (\alpha, \beta, \gamma)$ ее изотопия.

Этап 1. Генерация ключей. Алисины ключи будут следующие:

Открытый ключ - это $(Q, f), T, T^{(m,n,k)} = (\alpha^m, \beta^n, \gamma^k)$, $m, n, k \in \mathbb{N}$, и алгоритм Марковского.

Закрытый ключ –это тройка чисел m, n, k.

Этап 2. Шифрование. Чтобы отправить сообщение $b \in (Q, f)$, Боб вычисляет $T^{(r,s,t)}, T^{(mr,ns,kt)}$ для случайных чисел $r, s, t \in \mathbb{N}$ и $(T^{(mr,ns,kt)}(Q, f))$. Шифротекст имеет вид: $(T^{(r,s,t)}, (T^{(mr,ns,kt)}(Q, f))b)$. Для шифрования Боб использует известный Алисе алгоритм Марковского.

Этап 3. Дешифрование. Алиса зная m, n, k, и получив шифротекст $(T^{(r,s,t)}, (T^{(mr,ns,kt)}(Q, f))b)$, вычисляет $(T^{(mr,ns,kt)}(Q, f))^{-1}$ используя $T^{(r,s,t)}$ и наконец она вычисляет b.

Пример 3.1. Пусть (Q, f) бинарная квазигруппа , задаваемая таблицей 1:

Таблица 1

∘	**1**	**2**	**3**	**4**	**5**
1	1	5	3	4	2
2	4	3	1	2	5
3	3	1	2	5	4
4	2	4	5	3	1
5	5	2	4	1	3

и $T = (\alpha, \beta, \gamma)$ ее изотопия, где: $\alpha = (1\ 4\ 3)\ (2\ 5)$, $\beta = (5\ 3\ 2)\ (1\ 4)$ и $\gamma = (1\ 4\ 5\ 2\ 3)$.

И для γ мы получим обратную подстановку γ^{-1} вида: $\gamma^{-1} = (3\ 2\ 5\ 4\ 1)$.

Для изотопии $T = (\alpha, \beta, \gamma)$ получим таблицу 2:

Этап 1.

Таблица 2.

$\alpha(\circ)$	**1**	**2**	**3**	**4**	**5**		$\beta(\circ)$	**1**	**2**	**3**	**4**	**5**		$\gamma(\circ)$	**1**	**2**	**3**	**4**	**5**
1	2	4	5	3	1		**1**	3	1	4	2	5		**1**	1	4	5	3	2
2	5	2	4	1	3		**2**	1	3	2	5	4		**2**	4	1	3	2	5
3	1	5	3	4	2		**3**	4	2	5	1	3		**3**	5	3	2	4	1
4	3	1	2	5	4		**4**	5	4	1	3	2		**4**	2	5	4	1	3
5	4	3	1	2	5		**5**	2	5	3	4	1		**5**	3	2	1	5	4

Генерация ключей. Ключи Алисы: секретный ключ: $m = 5, n = 5, k = 3$ и открытый ключ это $(Q, f), T, T^{(5,5,3)} = (\alpha^5, \beta^5, \gamma^3)$, где:

$$\alpha^5 = (1\ 3\ 4)\ (5\ 2);\ \ \beta^5 = (1\ 4)\ (2\ 3\ 5);\ \ \gamma^3 = (1\ 5\ 3\ 4\ 2)$$

и алгоритм Марковского.

Этап 2. Шифрование. Чтобы отправить сообщение b= 221543353 , Боб зная $T = (\alpha, \beta, \gamma)$:

$$\alpha = \begin{pmatrix} 1\ 2\ 3\ 4\ 5 \\ 4\ 5\ 1\ 3\ 2 \end{pmatrix};\ \ \beta = \begin{pmatrix} 1\ 2\ 3\ 4\ 5 \\ 4\ 5\ 2\ 1\ 3 \end{pmatrix};\ \ \gamma = \begin{pmatrix} 1\ 2\ 3\ 4\ 5 \\ 4\ 3\ 1\ 5\ 2 \end{pmatrix}$$

вычисляет $T^{(r,s,t)}$ для случайных $r = 2, s = 3, t = 4$, т.е. $T^{(2,3,4)}$:

$$\alpha^2 = \begin{pmatrix} 1\ 2\ 3\ 4\ 5 \\ 3\ 2\ 4\ 1\ 5 \end{pmatrix};\ \ \beta^3 = \begin{pmatrix} 1\ 2\ 3\ 4\ 5 \\ 4\ 2\ 3\ 1\ 5 \end{pmatrix};\ \ \gamma^4 = \begin{pmatrix} 1\ 2\ 3\ 4\ 5 \\ 3\ 5\ 2\ 1\ 4 \end{pmatrix}.$$

В нашем примере $T^{(2,3,4)}$: $\alpha^2 = (1\ 3\ 4)$; $\beta^3 = (1\ 4)$; $\gamma^4 = (1\ 3\ 2\ 5\ 4)$.

Затем он вычисляет $T^{(mr,ns,kt)}$ используя открытый ключ:

$$T^{(m,n,k)} = (\alpha^m, \beta^n, \gamma^k) = (\alpha^*, \beta^*, \gamma^*):$$

$$\alpha^* = \begin{pmatrix} 1\ 2\ 3\ 4\ 5 \\ 3\ 5\ 4\ 1\ 2 \end{pmatrix};\ \ \beta^* = \begin{pmatrix} 1\ 2\ 3\ 4\ 5 \\ 4\ 3\ 5\ 1\ 2 \end{pmatrix};\ \gamma^* = \begin{pmatrix} 1\ 2\ 3\ 4\ 5 \\ 2\ 4\ 5\ 3\ 1 \end{pmatrix}.$$

И возводя эти перестановки в соответствующие степени: $r = 2, s = 3, t = 4$ получает:

$$(\alpha^*)^2 = \begin{pmatrix} 1\ 2\ 3\ 4\ 5 \\ 4\ 2\ 1\ 3\ 5 \end{pmatrix};\ \ (\beta^*)^3 = \begin{pmatrix} 1\ 2\ 3\ 4\ 5 \\ 4\ 2\ 3\ 1\ 5 \end{pmatrix};\ (\gamma^*)^4 = \begin{pmatrix} 1\ 2\ 3\ 4\ 5 \\ 5\ 1\ 4\ 2\ 3 \end{pmatrix}$$

$$\alpha^{2m} = (\ 1\ 4\ 3)\ ;\ \ \beta^{3n} = (1\ 4)\ ;\ \ \gamma^{4k} = (1\ 5\ 3\ 4\ 2),\qquad (\gamma^{4k})^{-1} = (1\ 2\ 4\ 3\ 5).$$

В результате применения новой изотопии $T^{(2m,3n,4k)}$ к квазигруппе (Q, f) получаем:

Таблица 3.

$\alpha^{2m}(\circ)$	**1**	**2**	**3**	**4**	**5**	$\beta^{3n}(\circ)$	**1**	**2**	**3**	**4**	**5**	$(\gamma^{4k})^{-1}(\circ)$	**1**	**2**	**3**	**4**	**5**
1	2	4	5	3	1	**1**	3	4	5	2	1	**1**	5	3	1	4	2
2	4	3	1	2	5	**2**	2	3	1	4	5	**2**	4	5	2	3	1
3	1	5	3	4	2	**3**	4	5	3	1	2	**3**	3	1	5	2	4
4	3	1	2	5	4	**4**	5	1	2	3	4	**4**	1	2	4	5	3
5	5	2	4	1	3	**5**	1	2	4	5	3	**5**	2	4	3	1	5

Чтобы получить $(T^{(mr,ns,kt)}(Q, f)b$, Боб использует алгоритм Марковского известный Алисе, зная значение лидера $l = 1$. Тогда шифротекст для сообщения

b = 221543353 будет иметь вид:

$$v_1 = 1 \circ 2 = 3,$$
$$v_2 = 3 \circ 2 = 1,$$
$$v_3 = 1 \circ 1 = 5,$$
$$v_4 = 5 \circ 5 = 5,$$
$$v_5 = 5 \circ 4 = 1,$$

$$v_6 = 1 \circ 3 = 1,$$
$$v_7 = 1 \circ 3 = 1,$$
$$v_8 = 1 \circ 5 = 2,$$
$$v_9 = 2 \circ 3 = 2,$$

В результате получен шифротекст вида: $b' = 315511122$.

Этап 3. Дешифрование. Алиса зная $m = 5, n = 5, k = 3$, получив изотопию $T^{(r,s,t)}$ и шифротекст $(T^{(mr,ns,kt)}(Q,f))b) = 315511122$, сначала вычислит изотопию $T^{(mr,ns,kt)}$ используя $T^{(r,s,t)} = T^{(**,**,**)}$:

$$\alpha^{**} = \begin{pmatrix} 1\,2\,3\,4\,5 \\ 3\,2\,4\,1\,5 \end{pmatrix};\ \beta^{**} = \begin{pmatrix} 1\,2\,3\,4\,5 \\ 4\,2\,3\,1\,5 \end{pmatrix};\ \gamma^{**} = \begin{pmatrix} 1\,2\,3\,4\,5 \\ 3\,5\,2\,1\,4 \end{pmatrix}.$$

Она вычисляет $T^{(mr,ns,kt)}$:

$$(\alpha^{**})^5 = \begin{pmatrix} 1\,2\,3\,4\,5 \\ 4\,2\,1\,3\,5 \end{pmatrix};\ (\beta^{**})^5 = \begin{pmatrix} 1\,2\,3\,4\,5 \\ 4\,2\,3\,1\,5 \end{pmatrix};\ (\gamma^{**})^3 = \begin{pmatrix} 1\,2\,3\,4\,5 \\ 5\,1\,4\,2\,3 \end{pmatrix}$$

В результате она получает такую же таблицу Кэли (таблицу 3). Для $(\gamma^{4k})^{-1}$ строит парастроф (23), который используется в алгоритме Марковского для дешифрования:

Таблица 4

\	**1**	**2**	**3**	**4**	**5**
1	3	5	2	4	1
2	5	3	4	1	2
3	2	4	1	5	3
4	1	2	5	3	4
5	4	1	3	2	5

И применяя таблицу 4 для $b' = 315511122$ восстанавливает b:

$$u_1 = 1\backslash 3 = 2,$$
$$u_2 = 3\backslash 1 = 2,$$
$$u_3 = 1\backslash 5 = 1,$$
$$u_4 = 5\backslash 5 = 5,$$
$$u_5 = 5\backslash 1 = 4,$$
$$u_6 = 1\backslash 1 = 3,$$
$$u_7 = 1\backslash 1 = 3,$$
$$u_8 = 1\backslash 2 = 5,$$
$$u_9 = 2\backslash 2 = 3.$$

В результате исходный текст был восстановлен: $b = 221543353$.

В этом алгоритме изострофия [6] может использоваться вместо изотопии. Вместо бинарных квазигрупп можно использовать левосторонние и правосторонние квазигруппы, либо $n-$арные ($n > 2$) квазигруппы [7; 8]. И как следствие последнего вместо алгоритма Марковского будут использованы его обобщенные алгоритмы на соответствующие квазигруппы. Из всех возможных модификаций предстоит выбрать вариант наиболее стойкий ко всем видам известных на текущий момент атак.

Заключение

Сегодня разные точки зрения на одну и ту же математическую идею приводят к разным обобщениям. В своей работе мы рассмотрели аналог системы шифрования Эль-Гамаля на основе алгоритма Марковского. Этот алгоритм находится в стадии разработки и совершенствования.

Используемые источники:

1. ELGAMAL, T. *A public key cryptosystem and a signature scheme based on discrete logarithms*. - IEEE Transactions on Information Theory, 31(4): p.469-472, 1985.
2. RYABKO, B.YA.; FIONOV, A.N. *Cryptographic methods of information protection: a training manual*. - M. Hotline-Telecom, 2005, p. 12-34. ISBN 5-89176-233-1.
3. https://ru.wikipedia.org/wiki/Схема_Эль-Гамаля.
4. MOLDOVYAN, N.A.; SHCHERBACOV, A.V. and SHCHERBACOV, V.A. *On some applications of quasigroups in cryptology*. In Workshop on Foundations of Informatics, August 24-29, 2015, Chisinau, Proceedings, pages 331-341.
5. SHCHERBACOV, V.A. *On generalisation of Markovski cryptoalgorithm*. In Workshop on General Algebra, February 26-March 1, 2015, Technische Universitat at Dresden, Technical Report, Technische Universitat at Dresden, Dresden, 36-37, 2015.
6. SHCHERBACOV, V.A. *On the structure of left and right F-, SM- and E-quasigroups*. J. Gen. Lie Theory Appl., 3(3): p. 197-259, 2009.
7. БЕЛОУСОВ, В.Д. *n-арные квазигруппы*. Stiintsa, Кишинев, 1971.
8. SHCHERBACOV, V.A.. *Quasigroups in cryptology*. Comput. Sci. J. Moldova, 17(2): p. 193-228, 2009.

Conducător științific: Corlat Andrei - doctor, conferențiar universitar