ЕВКЛИДОВЫ КРИПТОСИСТЕМЫ

А. Б. Дюсенбина, В. Д. Тэн

Казахстанско-Британский технический университет,
050000, Алма-Ата, Республика Казахстан

УДК 512.54

Построена криптосистема без повторений. Предложенный алгоритм шифрования позволяет шифровать любой текст, так чтобы все символы после шифрования были различными. В данном случае методы статистического анализа даже теоретически не могут быть применены для взлома системы.

Ключевые слова: алфавит, повторение, евклидово кольцо, криптосистема, шифрование, расшифровка, атака.

In this paper we construct cryptosystems without repetitions. This means that the encryption algorithm can encrypt any text so that all symbols after encryption are different. Therefore, methods of statistic analysis can not be used against our cryptosystems even theoretically.

Key words: alphabet, repetition, Euclidean ring, cryptosystem, encryption, decryption, attack.

Введение. В настоящей работе используются некоторые термины и обозначения из работы [1]. Пусть Σ — конечное множество, называемое алфавитом. Элементы Σ называются буквами, конечная последовательность элементов множества Σ называется словом. Количество букв, входящих в слово w, есть длина слова w, множество всех слов Σ^* — пространство исходных текстов. Если X — множество, то $|X|$ обозначает количество элементов множества X. Число $|\Sigma|$ называется длиной алфавита Σ. Если Σ — некоторый алфавит, то исходный текст любого элемента Σ называется алфавитным исходным текстом (apt). Аналогично шифротекст любого элемента Σ называется алфавитным шифротекстом (act). Длина исходного текста (шифротекста) есть число алфавитных исходных текстов (шифротекстов), входящих в данный исходный текст (шифротекст).

Целью настоящей работы является построение криптосистем, удовлетворяющих следующим условиям:

А. Алгоритм шифрования позволяет шифровать исходные тексты любой длины, так чтобы после шифрования фиксированным ключом (конечным числом ключей) все алфавитные шифротексты были различными, т. е. чтобы зашифрованный текст не содержал повторений. Длина алфавита ограничена длиной ключа.

Б. Алгоритм шифрования позволяет шифровать исходные тексты любой длины, так чтобы после шифрования фиксированным ключом (конечным числом ключей) все алфавитные шифротексты были различными. Длина алфавита не ограничена.

В условиях А, Б наиболее важными являются выражения “любой длины” и “фиксированным ключом”, так как известны другие криптосистемы без повторений, или полиалфавитные криптосистемы, к числу которых относятся, например, системы CBC и CTR [2]. Однако если длина ключа зафиксирована, то длина текста без повторений ограничена.

Предположим, что имеется шифротекст большой длины. Тогда одним из методов нахождения алфавитных исходных текстов является статистический анализ, основанный на

распределении частот элементов алфавита. Очевидно, что если криптосистема удовлетворяет условию А или Б, то этот метод неприменим даже теоретически.

1. Основная теорема. *Пусть K — евклидово кольцо* [3] *с неотрицательной функцией, принимающей целые значения:*

$$\delta : K \setminus \{0\} \to N \cup \{0\}.$$

Здесь N — множество всех натуральных чисел; функция δ удовлетворяет следующим условиям:

I. *Неравенство $\delta(ab) \geq \delta(a)$ имеет место для всех ненулевых элементов $a \in K, b \in K$.*

II. *Если $a \in K, b \in K$ и $b \neq 0$, то существуют элементы $q \in K, r \in K$, такие что $a = qb + r$, при этом либо $\delta(r) < \delta(b)$, либо $r = 0$.*

Если $a \in K, b \in K$, то $\gcd(a, b) = d$ есть наибольший общий делитель элементов a и b. Если e — единица кольца K, то элементы a, b взаимно просты при $\gcd(a, b) = e$.

Далее будем предполагать, что все евклидовы кольца удовлетворяют следующему условию:

III. *Пусть $c \in K$ и $\mathrm{id}(c) = cK$ — главный идеал кольца K, порожденный элементом c. Если элементы $a \in K, b \in K$ удовлетворяют условиям*

$$\delta(a) < \delta(c), \quad \delta(b) < \delta(c), \quad a - b \equiv 0 (\mathrm{mod}\ \mathrm{id}(c)),$$

то $a = b$.

Замечание 1. Примерами колец, удовлетворяющих условию III, являются кольцо целых чисел и кольца многочленов над полями. Примером кольца, которое не удовлетворяет условию III, является кольцо целых гауссовых чисел [3].

Алгоритмы шифрования и расшифровки построены на основе следующей теоремы.

Теорема 1. *Пусть K — евклидово кольцо, k — произвольный необратимый элемент K. Тогда для любого необратимого элемента $p \in K$, такого что $\delta(p) < \delta(k)$, и для любого элемента $s \in K$, такого что*

$$\gcd(s, k) = e, \quad \gcd(s, p) = e, \tag{1}$$

существуют элементы $a_p \in K, c \in K$, удовлетворяющие следующим условиям:

1) $\delta(a_p) < \delta(k)$;

2) $c = a_p s$, $c \equiv p (\mathrm{mod}\ \mathrm{id}(k))$, *где* $\mathrm{id}(k)$ *— главный идеал кольца K, порожденный элементом k*;

3) $\delta(k) < \delta(c)$;

4) *если $p_1 \neq p_2$ и $\delta(p_1) < \delta(k)$, $\delta(p_2) < \delta(k)$, то $c_1 \neq c_2$, и наоборот: если $c_1 \neq c_2$, то $p_1 \neq p_2$.*

Доказательство. Пусть k — элемент кольца K, p — элемент K и $\delta(p) < \delta(k)$. Так как $\gcd(s, k) = e$, то из китайской теоремы об остатках [4] следует существование элемента $b_p \in K$, такого что

$$b_p \equiv 0 (\mathrm{mod}\ \mathrm{id}(s)), \quad b_p \equiv p (\mathrm{mod}\ \mathrm{id}(k)), \tag{2}$$

где $\mathrm{id}(s)$ — главный идеал кольца K, порожденный элементом s; $b_p = pus$; элемент u может быть получен из равенства $us + vk = e$. Пусть a_p — остаток от деления элемента $d_p = pu$ на элемент k. Как известно, элемент b_p, удовлетворяющий условиям (2), определен неоднозначно, но из условия $\gcd(s, k) = e$ следует, что любые два элемента $d'_p = pu'$, $d''_p = pu''$ имеют одинаковые остатки при делении на k, т. е. остаток a_p определен однозначно. Действительно, предположим, что элементы b'_p, b''_p удовлетворяют условиям (2). Тогда имеем

$$b'_p - b''_p = d'_p s - d''_p s \equiv 0(\mathrm{mod\ id}(k)),$$

откуда следует $d'_p - d''_p \equiv 0(\mathrm{mod\ id}(k))$. Однако при

$$\delta(a'_p) < \delta(k), \quad \delta(a''_p) < \delta(k),$$
$$a'_p - a''_p = d'_p - d''_p \equiv 0(\mathrm{mod\ id}(k))$$

из условия III получаем равенство

$$a'_p = a''_p.$$

Нетрудно показать, что

$$b_p = d_p s \equiv a_p s(\mathrm{mod\ id}(k)) \equiv p(\mathrm{mod\ id}(k)). \tag{3}$$

Если $c = a_p s$, то из (3) следует, что c удовлетворяет условию 2 теоремы. Неравенство $\delta(k) < \delta(c)$ верно, так как иначе имеем

$$c = a_p s \equiv p(\mathrm{mod\ id}(k)), \quad \delta(p) < \delta(k), \quad \delta(c) < \delta(k).$$

Из условия III следует, что $c = a_p s = p$, но это невозможно, так как $\gcd(s, p) = e$, поэтому условие 3 выполнено. Из (2) следует, что если $\delta(p_1) < \delta(k)$, $\delta(p_2) < \delta(k)$ и $p_1 \neq p_2$, то $c_1 \neq c_2$, и если $c_1 \neq c_2$, то $p_1 \neq p_2$, поэтому выполняется условие 4.

2. Алгоритмы шифрования и расшифровки. Алгоритм шифрования C_1: пусть k — элемент евклидова кольца K, p — любой элемент K, такой что $\delta(k) < \delta(p)$, и s — любой элемент кольца K, удовлетворяющий условиям (1). Применяя теорему 1, получаем элемент c. Таким образом, k — секретный ключ, p — исходный текст, c — шифротекст.

Алгоритм расшифровки D_1: $p = c(\mathrm{mod}\ k)$, т. е. p — остаток от деления c на k.

Замечание 2. Так как множество неизоморфных евклидовых колец, удовлетворяющих условию III, бесконечно, то из теоремы 1 получаем бесконечное семейство различных криптосистем.

Замечание 3. В рассматриваемой криптосистеме нетрудно заменить секретный ключ. Действительно, если секретный ключ k поменять на k_1, то после шифрования получим новое значение шифротекста c_1, а после расшифровки — значение $p = c_1(\mathrm{mod}\ k_1)$.

Определение 1. Элемент $s \in K$ называется частичным ключом пары (k, p), если он удовлетворяет условиям (1). Если S является конечным множеством различных частичных ключей, то $|S|$ называется периодом S. Если множество S бесконечно, то период бесконечен.

Замечание 4. Пусть k — секретный ключ, p — исходный текст. Тогда из теоремы 1 следует, что для любого промежуточного ключа s можно построить шифротекст c_s, отличающийся от шифротекстов для других промежуточных ключей, но для всех s $p = c_s(\mathrm{mod}\ k)$.

Промежуточные ключи используются в процессе шифрования и не используются в процессе расшифровки.

Пусть K — евклидово кольцо, k — элемент кольца K, $p_1, p_2, ..., p_m$ — последовательность элементов K, таких что $\delta(p_i) < \delta(k)$. Предположим, что кольцо K удовлетворяет следующему условию: множество $S = \{s \in K, s$ — простой элемент, $\delta(s) > \delta(k)\}$ бесконечно.

Очевидно, что любой элемент множества S является частичным ключом любой пары (k, p_i). Пусть $s_1, s_2, ..., s_m$ — последовательность различных элементов S, тогда s_i является частичным ключом пары (k, p_i), $i = 1, 2, ..., m$. Из теоремы 1 следует, что если алгоритм шифрования C_1 применить к исходным текстам $p_1, p_2, ..., p_m$ с соответствующими частичными ключами $s_1, s_2, ..., s_m$, то все шифротексты $c_1, c_2, ..., c_m$ будут различными. Действительно, предположим, что

$$c_i = c_j, \quad i \neq j.$$

Из теоремы 1 следует, что $a_p^{(i)} s_i = a_p^{(j)} s_j$, $\delta(a_p^{(i)}) < \delta(k)$, $\delta(a_p^{(j)}) < \delta(k)$, а согласно условию, налагаемому на евклидово кольцо K, s_i, s_j — простые элементы, $\delta(s_i) > \delta(k), \delta(s_j) > \delta(k)$. Поэтому равенство $a_p^i s_i = a_p^j s_j$ невозможно, так как $\gcd(s_i, s_j) = \gcd(a_p^i, s_j) = e$.

Предположим, что евклидово кольцо K удовлетворяет сформулированному выше условию, налагаемому на евклидовы кольца. Тогда получаем следующие алгоритмы шифрования и расшифровки.

Алгоритм шифрования C_2: пусть k — элемент кольца K, $p_1, p_2, ..., p_m$ — последовательность элементов K, таких что $\delta(p_i) < \delta(k), i = 1, ..., m, s_1, s_2, ..., s_m$ — последовательность различных элементов S. Зашифруем элемент p_i, используя частичный ключ s_i и алгоритм C_1. В результате все шифротексты $c_1, c_2, ..., c_m$ будут различными. Таким образом, k — секретный ключ, $p_1, p_2, ..., p_m$ — последовательность исходных текстов, $s_1, s_2, ..., s_m$ — последовательность соответствующих частичных ключей, $c_1, c_2, ..., c_m$ — соответствующие шифротексты.

Алгоритм расшифровки D_2: $p_i = c_i (\mathrm{mod}\ k), i = 1, 2, ..., m$.

Ниже описаны криптосистемы, обладающие свойствами А и Б.

Теорема 2. *Пусть $K = Z$ — кольцо целых чисел. Тогда криптосистема с алгоритмом шифрования* C_2 *и алгоритмом расшифровки* D_2 *удовлетворяет условию* А.

Доказательство. Известно, что Z является евклидовым кольцом с функцией $\delta(z) = |z|$, $z \in Z$ и Z удовлетворяет условию, налагаемому на евклидовы кольца. Если k — секретный ключ рассматриваемой криптосистемы, то из теоремы 1 следует, что число различных алфавитных исходных текстов не превышает числа $2|k|$. Поэтому данная криптосистема удовлетворяет свойству А.

Теорема 3. *Пусть $K = Q[x]$ — кольцо многочленов над полем рациональных чисел Q. Тогда криптосистема с алгоритмом шифрования* C_2 *и алгоритмом расшифровки* D_2 *удовлетворяет условию* Б.

Доказательство. Кольцо $Q[x]$ является евклидовым кольцом с функцией $\delta(f) = \deg f$, $f \in Q[x]$ и удовлетворяет условию, налагаемому на евклидовы кольца. Пусть $k \in q[x]$ является секретным ключом данной криптосистемы и $\deg k \geq 2$, тогда очевидно, что множество многочленов $g \in Q[x]$, таких что $\deg g < \deg k$, бесконечно. Поэтому рассматриваемая криптосистема удовлетворяет требованию Б.

3. Атаки и модификация алгоритмов. Рассмотрим следующую атаку с известным исходным текстом.

Предположение 1. Предположим, что известны исходные тексты $p_1, p_2, ..., p_n$ и соответствующие им шифротексты $c_1, c_2, ..., c_n$. Как и выше, обозначим через k секретный ключ. Из алгоритма расшифровки следует, что существуют элементы $d_1, ..., d_n \in K$, такие что

$$a_i = c_i - p_i = d_i k, \quad i = 1, 2, ..., n.$$

Обозначим через $\gcd(x_1, ..., x_n)$ наибольший общий делитель элементов $x_1, x_2, ..., x_n \in K$. Тогда имеем

$$\gcd(a_1, ..., a_n) = dk, \quad d = \gcd(d_1, ..., d_n).$$

Эта атака может привести к нахождению секретного ключа k.

Предлагается следующая модификация алгоритмов шифрования и расшифровки криптосистемы.

Алгоритм шифрования C_3: пусть $a \in K, b \in K, \delta(b) < \delta(ak), \gcd(a, b) \neq e$ и

$$\overline{c} = (q; r) \in K \times K,$$

где $ac = bq + r$ и $ac \neq r$, так как $\delta(c) > \delta(k)$. Рассмотрим два отображения $E_k : K \to K$ и $\overline{E}_{a,b} : K \to K \times K$, которые определены следующим образом:

$$E_k(p) = c, \quad \overline{E}_{a,b}(c) = (q, r).$$

Тогда

$$\overline{c} = \overline{E}_{a,b}(E_k(p)).$$

Имеем: p — исходный текст, $\overline{c}$ — шифротекст. Сначала используем алгоритм C_2, затем — отображение $\overline{E}_{a,b}$.

Алгоритм расшифровки D_3:

$$[a^{-1}(bq + r)](\mathrm{mod}\ k) = p.$$

Элемент a^{-1} является элементом поля частных кольца K, причем элемент $a^{-1}(bq + r) \in K$. В данном случае имеем три секретных ключа: k, a, b. Исходный текст является элементом кольца K, шифротекст — элементом декартова произведения $K \times K$. Очевидно, что если криптосистема с алгоритмом шифрования C_2 и алгоритмом расшифровки D_2 удовлетворяет требованию А или Б, то криптосистема с алгоритмами C_3 и D_3 удовлетворяет тому же требованию.

Определение 2. Шифры, в алгоритм шифрования которых входит алгоритм C_2, а в алгоритм расшифровки — алгоритм D_2, будем называть евклидовыми шифрами.

Замечание 5. Евклидовы шифры относятся к классу блочных шифров.

Теперь можно объяснить причину введения двух дополнительных ключей a, b и условия $\gcd(a, b) \neq e$.

Предположение 2. Предположим, что введен один дополнительный ключ a. Следовательно, имеется два секретных ключа k и a. Тогда

$$\overline{c} = ac.$$

Если для некоторого $1 \leq i \leq n$ имеется последовательность шифротекстов $\overline{c_1}, \overline{c_2}, ..., \overline{c_n}$ и $\gcd(a, c_i) = 1$, то

$$\gcd(\overline{c_1}, \overline{c_2}, ..., \overline{c_n}) = da, \quad d = \gcd(c_1, c_2, ..., c_n).$$

Если $d = 1$, то находим a, а значит, $c_1, c_2, ..., c_n$. Следовательно, можно применить атаку с исзвестным исходным текстом.

Предположение 3. Предположим, что введен один дополнительный ключ b. Тогда имеем два секретных ключа k и b. В этом случае

$$c = qb + r.$$

Если имеется две пары исходных текстов и соответствующих им шифротекстов $p_1, c_1 = (q_1, r_1)$ и $p_2, c_2 = (q_2, r_2)$, то

$$\begin{aligned} c_1 &= q_1 b + r_1, \\ c_2 &= q_2 b + r_2, \\ c_1 - p_1 &= q_1 b + r_1 - p_1, \\ c_2 - p_2 &= q_2 b + r_2 - p_2. \end{aligned} \tag{4}$$

Умножая первое равенство в (4) на q_2, второе — на q_1 и вычитая из первого равенства второе, для некоторого элемента $d \in K$ получаем

$$q_2(r_1 - p_1) - q_1(r_2 - p_2) = q_2(c_1 - p_1) - q_1(c_2 - p_2) = dk.$$

Таким образом, имея некоторое множество пар исходных текстов и соответствующих им шифротекстов, вновь можно применить атаку с известным исходным текстом.

Предположение 4. Предположим, что имеется три секретных ключа k, a, b, но $\gcd(a, b) = e$. Тогда, рассматривая две пары исходных текстов и соответствующих им шифротекстов $p_1, c_1 = (q_1, r_1)$ и $p_2, c_2 = (q_2, r_2)$, имеем

$$c_1 - ap_1 = q_1 b + r_1 - ap_1,$$

$$c_2 - ap_2 = q_2 b + r_2 - ap_2.$$

Умножая первое равенство на r_2, второе — на r_1 и вычитая из первого равенства второе, для некоторого $d \in K$ получаем

$$b(q_1 r_2 - q_2 r_1) - a(p_1 r_2 - p_2 r_1) = dak.$$

Если $\gcd(a, b) = e$, то $q_1 r_2 - q_2 r_1$ делится на a. Поэтому, имея некоторое множество пар шифротекстов $(q_1, r_1), ..., (q_{2m}, r_{2m})$, для некоторого $d_1 \in K$ получаем

$$\gcd(q_1 r_2 - q_2 r_1, ..., q_{2m-1} r_{2m} - q_{2m} r_{2m-1}) = d_1 a.$$

Эта атака может быть эффективна при нахождении a. Криптоанализ предлагаемых систем может быть продолжен при изучении евклидовых криптосистем для конкретных евклидовых колец, таких как кольцо целых чисел Z и кольца многочленов над полем. В частности, для криптосистем можно использовать методы дифференциального и линейного криптоанализа [5–7].

Список литературы

1. Salomaa A. Public-key cryptography. S. l.: Springer-Verlag, 1990.

2. Шнайер Б. Прикладная криптография. М.: Триумф, 2003.

3. Van der Waerden B. L. Algebra 1. S. l.: Springer-Verlag, 1971.

4. Lang S. Algebra. S. l.: Addison-Wesley Publ. Co., 1965.

5. Biham E. Differential cryptanalysis of the Data Encryption Standard / E. Biham, A. Shamir. S. l.: Springer-Verlag, 1993.

6. Агибалов Г. П. Элементы теории дифференциального криптоанализа итеративных блочных шифров с аддитивным раундовым ключом // Прикл. дискрет. математика. 2008. № 1. С. 34–42.

7. Matsui M. Linear cryptanalysis of DES cipher (1) // Proc. of the 1993 Symp. on cryptography and information security, Japan, Jan. 28–30, 1993. S. l. P. 1–14.

Дюсенбина Айжан Бекеевна — канд. физ.-мат. наук, ассоциированный проф. Казахстанско-Британского технического университета; e-mail: dusenbina_a@mail.ru;

Тэн Владимир Дянчунович — канд. физ.-мат. наук, ассоциированный проф., Казахстанско-Британского технического университета; e-mail: tenvd@mail.ru

Дата поступления — 27.03.13