УДК 519.7 DOI: 10.14529/mmp140206

О СОВЕРШЕННЫХ ШИФРАХ НА ОСНОВЕ ОРТОГОНАЛЬНЫХ ТАБЛИЦ

С.М. Рацеев, О.И. Череватенко

В работе исследуются совершенные шифры, стойкие к имитации и подмене шифрованных сообщений. Особо выделен случай, когда вероятности имитации и подмены достигают нижних границ. Хорошо известно, что шифр гаммирования с равновероятной гаммой является совершенным, но максимально уязвимым к попыткам имитации и подмены. Это происходит потому, что в шифре гаммирования алфавиты для записи открытых и шифрованных текстов равномощны. Так как одним из недостатков математической модели шифра являются ограничения, накладываемые на мощности множеств открытых текстов и ключей, то сначала приводится математическая модель шифра замены с неограниченным ключом, предложенная А.Ю. Зубовым. На основе данной модели в работе приводятся конструкции совершенных шифров, стойких к имитации и подмене. Данные шифры строятся на основе ортогональных таблиц и латинских прямоугольников. Рассматривается случай, когда случайный генератор ключевых последовательностей не обязательно имеет равномерное распределение вероятностей. Так как длины ключей таких шифров не меньше длин передаваемых сообщений, то шифры замены с неограниченным ключом целесообразно использовать в исключительно важных случаях.

Ключевые слова: шифр; совершенный шифр; имитация сообщения.

Введение

К. Шеннон в 40-х годах XX-го века ввел понятие совершенного шифра, обеспечивающего наилучшую защиту открытых текстов. Такой шифр не дает криптоаналитику никакой дополнительной информации об открытом тексте на основе перехваченной криптограммы. Данные шифры используются в тех случаях, когда наиболее важна секретность передаваемой информации. Наиболее хорошо известным совершенным шифром является шифр гаммирования с равновероятной гаммой. При этом данный шифр максимально уязвим к попыткам имитации и подмены шифрованных сообщений и строится с помощью генератора ключевых последовательностей с равномерным распределением. В данной работе рассматриваются задачи построения совершенных шифров, стойких к имитации и подмене шифрованных сообщений.

Напомним несколько важных определений.

Латинским квадратом s-го порядка над множеством $Y = \{y_1, ..., y_s\}$ называется таблица размера $s \times s$, заполненная элементами множества Y таким образом, что в каждой строке и в каждом столбце каждый элемент встречается ровно один раз.

Две матрицы $A = (a_{ij})$ и $B = (b_{ij})$ над множеством $Y = \{y_1, ..., y_s\}$ называются *ортогональными*, если все упорядоченные пары (a_{ij}, b_{ij}) различны.

Ортогональной таблицей $OA(s, n)$ над множеством $Y = \{y_1, ..., y_s\}$ называется матрица размера $s^2 \times n$ над множеством Y с тем условием, что для любых двух столбцов данной матрицы каждая из пар $(y_i, y_j) \in Y \times Y$ встречается ровно один раз. Существование ортогональной таблицы $OA(s, n)$ над множеством Y эквивалентно существованию n попарно ортогональных квадратных матриц порядка s над множеством Y [1].

Хорошо известно, что если число s является степенью некоторого простого числа, то в этом случае существуют $s - 1$ попарно ортогональных латинских квадрата, или, что то-

же самое, $s+1$ ортогональных матриц [2]: для этого достаточно рассмотреть многочлены $f_\alpha(x,y)=\alpha x+y$ над полем $GF(s)$ при ненулевых α.

Будем говорить, что матрица $A=A(s,n)$, $s\geq n$, над некоторым s-элементным множеством Y является *латинским прямоугольником*, если каждый столбец матрицы A является перестановкой элементов множества Y, причем в строках каждый элемент встречается не более одного раза.

1. Шифры замены с неограниченным ключом

Рассмотрим математическую модель шифра замены с неограниченным ключом, предложенную А.Ю. Зубовым [3]. Такая математическая модель имеет ряд полезных свойств, например, она позволяет строить модели совершенных шифров и кодов аутентификации, стойких к имитации и подмене (см. [4, 5, 6]).

Пусть U — конечное множество возможных шифрвеличин, V — конечное множество возможных шифробозначений. Пусть также имеются $r>1$ инъективных отображений из U в V. Пронумеруем данные отображения: E_1, E_2,..., E_r. Данные отображения называются простыми заменами. Обозначим $\mathbb{N}_r=\{1,2,...,r\}$. Опорным шифром шифра замены назовем совокупность $\Sigma=(U,\mathbb{N}_r,V,E,D)$, для которой выполнены следующие свойства:

1) для любых $u\in U$ и $j\in\mathbb{N}_r$ выполнено равенство $D_j(E_j(u))=u$;

2) $V=\bigcup_{j\in\mathbb{N}_r}E_j(U)$.

При этом $E=\{E_1,...,E_r\}$, $D=\{D_1,...,D_r\}$, $D_j:E_j(U)\to U$, $j\in\mathbb{N}_r$.

l-й степенью опорного шифра Σ назовем совокупность

$$\Sigma^l=(U^l,\mathbb{N}_r^l,V^l,E^{(l)},D^{(l)}),$$

где $U^l,\mathbb{N}_r^l,V^l$ — декартовы степени соответствующих множеств U, $\mathbb{N}_r$, V. Множество $E^{(l)}$ состоит из отображений $E_{\overline{\jmath}}:U^l\to V^l$, $\overline{\jmath}\in\mathbb{N}_r^l$, таких, что любых $\overline{u}=u_1...u_l\in U^l$, $\overline{\jmath}=j_1...j_l\in\mathbb{N}_r^l$ выполнено равенство

$$E_{\overline{\jmath}}(\overline{u})=E_{j_1}(u_1)...E_{j_l}(u_l)=v_1...v_l\in V^l,$$

а множество $D^{(l)}$ состоит из отображений $D_{\overline{\jmath}}:E_{\overline{\jmath}}(U^l)\to U^l$, $\overline{\jmath}\in\mathbb{N}_r^l$, таких, что любых $\overline{v}=v_1...v_l\in V^l$, $\overline{\jmath}=j_1...j_l\in\mathbb{N}_r^l$ выполнено равенство

$$D_{\overline{\jmath}}(\overline{v})=D_{j_1}(v_1)...D_{j_l}(v_l)=u_1...u_l\in U^l.$$

Пусть ψ_c — случайный генератор ключевого потока, который для любого натурального числа l вырабатывает случайный ключевой поток $j_1...j_l$, где все $j_i\in\mathbb{N}_r$.

Обозначим через Σ_H^l следующую совокупность величин:

$$\Sigma_H^l=(U^l,\mathbb{N}_r^l,V^l,E^{(l)},D^{(l)},P_{U^l},P_{\mathbb{N}_r^l}).$$

Шифром замены с неограниченным ключом назовем семейство

$$\Sigma_H=(\Sigma_H^l,\ l\in\mathbb{N};\ \psi_c).$$

При этом независимые и не содержащие нулевых вероятностей распределения P_{U^l} и $P_{\mathbb{N}_r^l}$ индуцируют распределения вероятностей на множестве V^l:

$$P_{V^l}(\overline{v})=\sum_{\substack{(\overline{u},\overline{\jmath})\in U^l\times\mathbb{N}_r^l\\ E_{\overline{\jmath}}(\overline{u})=\overline{v}}}P_{U^l}(\overline{u})\cdot P_{\mathbb{N}_r^l}(\overline{\jmath}).$$

Также определим условные вероятности $P_{U^l|V^l}(\overline{u}|\overline{v})$ и $P_{V^l|U^l}(\overline{v}|\overline{u})$:

$$P_{V^l|U^l}(\overline{v}|\overline{u}) = \sum_{\overline{\jmath}\in\mathbb{N}_r^l(\overline{u},\overline{v})} P_{\mathbb{N}_r^l}(\overline{\jmath}), \qquad P_{U^l|V^l}(\overline{u}|\overline{v}) = \frac{P_{U^l}(\overline{u})\cdot P_{V^l|U^l}(\overline{v}|\overline{u})}{P_{V^l}(\overline{v})},$$

где $\mathbb{N}_r^l(\overline{u},\overline{v}) = \{\overline{\jmath}\in\mathbb{N}_r^l \mid E_{\overline{\jmath}}(\overline{u}) = \overline{v}\}$.

Говорят, что шифр Σ_H является *совершенным*, если для любого натурального l и для любых $\overline{u}\in U^l$, $\overline{v}\in V^l$ выполнено равенство $P_{U^l|V^l}(\overline{u}|\overline{v}) = P_{U^l}(\overline{u})$. Приведем эквивалентные условия совершенного шифра.

Предложение 1. *Для шифра Σ_H следующие условия эквивалентны:*

(i) для любого $l\in\mathbb{N}$ и любых $\overline{u}\in U^l$, $\overline{v}\in V^l$ выполнено равенство $P_{U^l|V^l}(\overline{u}|\overline{v}) = P_{U^l}(\overline{u})$;

(ii) для любого $l\in\mathbb{N}$ и любых $\overline{u}\in U^l$, $\overline{v}\in V^l$ выполнено равенство $P_{V^l|U^l}(\overline{v}|\overline{u}) = P_{V^l}(\overline{v})$;

(iii) для любого $l\in\mathbb{N}$ и любых $\overline{u}_1,\overline{u}_2\in U^l$, $\overline{v}\in V^l$ выполнено равенство $P_{V^l|U^l}(\overline{v}|\overline{u}_1) = P_{V^l|U^l}(\overline{v}|\overline{u}_2)$.

Приведем также критерий совершенных шифров замены с неограниченным ключом в классе шифров с равномерным распределением вероятностей на множестве $\mathbb{N}_r$ из работы [5], который нам понадобится в дальнейшем.

Теорема 1. *Шифр Σ_H с равномерным распределением вероятностей $P_{\mathbb{N}_r}$ является совершенным тогда и только тогда, когда выполнены следующие условия:*

(i) для любых $u\in U$ и $v\in V$ найдется такое $j\in\mathbb{N}_r$, что $E_j(u) = v$;

(ii) для любых $u_1,u_2\in U$, $v\in V$ выполнено равенство $|\mathbb{N}_r(u_1,v)| = |\mathbb{N}_r(u_2,v)|$.

2. Имитация и подмена сообщений

Рассмотрим вероятностное пространство $(\Omega = \mathbb{N}_r, F_{\mathbb{N}_r}, P_{\mathbb{N}_r})$. Зафиксируем $v\in V$. Обозначим через $\mathbb{N}_r(v)$ следующее множество:

$$\mathbb{N}_r(v) = \{j\in\mathbb{N}_r \mid v\in E_j(U)\}.$$

Под обозначением $\mathbb{N}_r(v)$ будем также понимать событие $(\mathbb{N}_r(v)\in F_{\mathbb{N}_r})$, заключающееся в том, что при случайном выборе элемента $j\in\mathbb{N}_r$ шифробозначение v можно расшифровать правилом расшифрования D_j: $v\in E_j(U)$. Тогда событию $\mathbb{N}_r(v)$ будут благоприятствовать все элементы из множества $\mathbb{N}_r(v)$, и только они. Поэтому

$$P(\mathbb{N}_r(v)) = \sum_{j\in\mathbb{N}_r(v)} P_{\mathbb{N}_r}(j).$$

Если канал связи готов к работе, и на приеме установлены действующие ключи, но в данный момент времени никакого сообщения не передается, то в этом случае противником может быть предпринята попытка имитации сообщения. Тогда вероятность успеха имитации каждого символа передаваемого сообщения определяется следующим образом:

$$P_{im} = \max_{v\in V} P(\mathbb{N}_r(v)).$$

Если же в данный момент передается некоторое сообщение, то противник может заменить некоторые символы этого сообщения, например, некоторый символ $v\in V$ на $\widetilde{v}\in V$, отличный от v. При этом он будет рассчитывать на то, что на действующем ключе шифробозначение $\widetilde{v}$ будет успешно расшифровано. Пусть «$\mathbb{N}_r(\widetilde{v}) \mid \mathbb{N}_r(v)$» — событие, заключающееся в

попытке подмены шифробозначения v шифробозначением $\widetilde{v}$. Применяя теорему о произведении вероятностей, получаем, что

$$P(\mathbb{N}_r(\widetilde{v}) \mid \mathbb{N}_r(v)) = \frac{P(\mathbb{N}_r(v) \cap \mathbb{N}_r(\widetilde{v}))}{P(\mathbb{N}_r(v))} = \frac{\sum_{j \in \mathbb{N}_r(v,\widetilde{v})} P_{\mathbb{N}_r}(j)}{\sum_{j \in \mathbb{N}_r(v)} P_{\mathbb{N}_r}(j)},$$

где $\mathbb{N}_r(v,\widetilde{v}) = \mathbb{N}_r(v) \cap \mathbb{N}_r(\widetilde{v})$. Тогда вероятность успеха подмены шифробозначения будет вычисляться по следующей формуле:

$$P_{podm} = \max_{\substack{v,\widetilde{v} \in V \\ v \neq \widetilde{v}}} P(\mathbb{N}_r(\widetilde{v}) \mid \mathbb{N}_r(v)).$$

Обозначим через P_{im}^l вероятность успеха имитации сообщения для шифра Σ_H^l, а через $P_{podm}^l(s)$ — вероятность успеха подмены в сообщении длины l ровно s символов для шифра Σ_H^l, где $s \leq l$. Из определения вероятностей P_{im} и P_{podm} следуют такие равенства:

$$P_{im}^l = (P_{im})^l, \quad P_{podm}^l(s) = (P_{podm})^s.$$

Пусть Σ_H — некоторый шифр замены с неограниченным ключом с опорным шифром $\Sigma = (U, \mathbb{N}_r, V, E, D)$, $|U| = n$, $|V| = s$, распределением вероятностей $P_{\mathbb{N}_r}$ для случайного генератора ψ_c и матрицей зашифрования A размера $r \times n$ над множеством V для опорного шифра Σ. При этом строки матрицы A пронумерованы элементами множества $\mathbb{N}_r$, а столбцы — элементами множества U. Пусть также для некоторого $\widetilde{r} \geq r$ имеется случайный генератор $\widetilde{\psi}_c$ с распределением вероятностей $P_{\mathbb{N}_{\widetilde{r}}}$ и условием, что найдется такое разбиение множества $\mathbb{N}_{\widetilde{r}}$ на r непустых непересекающиеся подмножеств

$$\mathbb{N}_{\widetilde{r}} = K_1 \cup K_2 \cup ... \cup K_r,$$

для которого выполнены равенства

$$P_{\mathbb{N}_{\widetilde{r}}}(K_i) = \sum_{k \in K_i} P_{\mathbb{N}_{\widetilde{r}}}(k) = P_{\mathbb{N}_r}(i), \quad i = 1, ..., r.$$

Построим шифр замены с неограниченным ключом $\widetilde{\Sigma}_H$ со случайным генератором $\widetilde{\psi}_c$ и опорным шифром $\widetilde{\Sigma} = (U, \mathbb{N}_{\widetilde{r}}, V, \widetilde{E}, \widetilde{D})$ со значениями U и V, как в опорном шифре Σ. Для этого необходимо определить множество правил зашифрования $\widetilde{E}$ и множество правил расшифрования $\widetilde{D}$. $\widetilde{E}$ и $\widetilde{D}$ определим с помощью матрицы зашифрования B размера $\widetilde{r} \times n$ над множеством V, в которой строки пронумерованы элементами множества $\mathbb{N}_{\widetilde{r}}$, а столбцы — элементами множества U, следующим образом: j-ю строку матрицы A продублируем $|K_j|$ раз, $j = 1, ..., r$, и из всех полученных (продублированных) строк составим матрицу B.

Предложение 2. *Если один из шифров Σ_H или $\widetilde{\Sigma}_H$ является совершенным, то другой также будет являться совершенным. Более того, вероятности успехов имитации и успехов подмены данных шифров соответственно равны.*

Доказательство следует из предложения 1 и определения понятий имитации и подмены.

3. Совершенные имитостойкие шифры

Пусть для чисел s и n, $1 < n < s$, существует ортогональная таблица $OA(s,n)$ над множеством $V = \{v_1, ..., v_s\}$, в которой i-я строка содержит только элемент v_i, $i = 1, ..., s$. Из сказанного выше следует, что если, например, s является степенью простого числа, то

$OA(s,n)$ существует для любого $n = 2, ..., s-1$. Вычеркнем из таблицы $OA(s,n)$ первые s строк и обозначим полученную таблицу через $A(s,n)$. Понятно, что таблица $A(s,n)$ имеет размерность $(s^2-s)\times n$, в каждой строке нет повторяющихся элементов, а каждый столбец содержит ровно $s-1$ экземпляров элемента v_i, $i = 1, ..., s$.

Теорема 2. *Пусть для шифра Σ_H выполнены следующие условия:*

(i) $|U| = n$, $|V| = s$, $1 < n < s$, $r = s^2 - s$;

(ii) матрица зашифрования опорного шифра представляет собой таблицу вида $A(s,n)$;

(iii) распределение вероятностей $P_{\mathbb{N}_r}$ является равномерным.

Тогда шифр Σ_H является совершенным, и для любого l выполнены следующие равенства:

$$P_{im}^l = \left(\frac{n}{s}\right)^l, \quad P_{podm}^l(t) = \left(\frac{n-1}{s-1}\right)^t,$$

то есть $P_{im}^l \to 0$ при $l \to \infty$, $P_{podm}^l(t) \to 0$ при $t \to \infty$.

Доказательство. Совершенность шифра Σ_H следует из теоремы 1.

Пусть $v \in V$. Тогда

$$P(\mathbb{N}_r(v)) = \frac{n(s-1)}{s(s-1)} = \frac{n}{s},$$

поэтому

$$P_{im}^l = \left(\frac{n}{s}\right)^l.$$

Пусть $v, \widetilde{v} \in V$, $v \neq \widetilde{v}$. Тогда

$$P(\mathbb{N}_r(\widetilde{v}) \mid \mathbb{N}_r(v)) = \frac{2C_n^2}{n(s-1)} = \frac{n-1}{s-1},$$

поэтому

$$P_{podm}^l(t) = \left(\frac{n-1}{s-1}\right)^t.$$

□

Заметим, что совершенные имитостойкие шифры можно строить не только для случая, когда $P_{\mathbb{N}_r}$ равномерно. Пусть

$$\mathbb{N}_r = K_1 \cup K_2 \cup ... \cup K_s \tag{1}$$

— разбиение множества $\mathbb{N}_r$ на непустые непересекающиеся подмножества с условием, что

$$P_{\mathbb{N}_r}(K_i) = \sum_{k \in K_i} P_{\mathbb{N}_r}(k) = \frac{1}{s}, \quad i = 1, ..., s. \tag{2}$$

Пусть $U = \{u_1, ..., u_n\}$, A — матрица размера $s \times n$, $1 < n < s$, над множеством $V = \{v_1, ..., v_s\}$ вида

v_1	v_2	...	v_n
v_2	v_3	...	v_{n+1}
...	...	...	...
v_s	v_1	...	v_{n-1}

,

в которой каждый следующий столбец является циклическим сдвигом на одну позицию предыдущего столбца. Понятно, что данная матрица является латинским прямоугольником. Как и перед предложением 2, на основе матрицы A построим матрицу зашифрования B размера $r \times n$ над множеством V для опорного шифра Σ.

Предложение 3. *Полученный шифр Σ_H будет являться совершенным, причем будут выполнены следующие равенства:*

$$P_{im}^{l} = \left(\frac{n}{s}\right)^{l}, \quad P_{podm}^{l}(t) = \left(\frac{n-1}{n}\right)^{t}.$$

Доказательство следует из предложения 2 и работы [4].

Пример 1. Пусть $U = \{u_1, u_2\}$, $V = \{v_1, v_2, v_3\}$, $\mathbb{N}_5 = \{1, 2, 3, 4, 5\}$, и распределение вероятностей на множестве $\mathbb{N}_5$ имеет вид

$\mathbb{N}_5$	1	2	3	4	5
$P_{\mathbb{N}_5}$	1/15	4/15	1/12	1/4	1/3

.

В этом случае существует разбиение вида (1) с условием (2):

$$K_1 = \{1, 2\},\ K_2 = \{3, 4\},\ K_3 = \{5\},$$

$$P_{\mathbb{N}_5}(K_1) = P_{\mathbb{N}_5}(K_2) = P_{\mathbb{N}_5}(K_3) = \frac{1}{3}.$$

Сначала составим матрицу A

$\mathbb{N}_3 \diagdown U$	u_1	u_2
1	v_1	v_2
2	v_2	v_3
3	v_3	v_1

,

которая является латинским прямоугольником, а на ее основе составим матрицу B

$\mathbb{N}_5 \diagdown U$	u_1	u_2
1	v_1	v_2
2	v_1	v_2
3	v_2	v_3
4	v_2	v_3
5	v_3	v_1

.

По предложению 3 для данных U, V, $\mathbb{N}_5$, $P_{\mathbb{N}_5}$ и матрицы зашифрования B для опорного шифра полученный шифр Σ_H будет являться совершенным, причем

$$P_{im}^{l} = \left(\frac{2}{3}\right)^{l}, \quad P_{podm}^{l}(t) = \left(\frac{1}{2}\right)^{t}.$$

Пусть теперь

$$\mathbb{N}_r = K_1 \cup K_2 \cup ... \cup K_{s^2-s} \tag{3}$$

— разбиение множества $\mathbb{N}_r$ с условием, что

$$P_{\mathbb{N}_r}(K_i) = \sum_{k \in K_i} P_{\mathbb{N}_r}(k) = \frac{1}{s^2 - s}, \quad i = 1, ..., s^2 - s. \tag{4}$$

Пусть T^j — циклическая перестановка на j позиций влево s-го множества. Обозначим через $A_j = A_j(s, 2)$ матрицу размера $s \times 2$ над множеством $V = \{v_1, ..., v_s\}$, имеющую такой вид:

$$A_j = \begin{pmatrix} v_1 & v_2 & ... & v_s \\ v_{T^j(1)} & v_{T^j(2)} & ... & v_{T^j(s)} \end{pmatrix}^T, \quad j = 1, ..., s-1.$$

Из матриц A_j, $j = 1, ..., s-1$, составим матрицу A размера $(s^2-s)\times 2$ путем последовательной графической записи матриц A_1,..., A_{s-1} одной под другой. Теперь на основе матрицы A построим матрицу зашифрования B размера $r \times 2$ для опорного шифра указанным выше способом.

Предложение 4. *Полученный шифр Σ_H будет являться совершенным, причем будут выполнены следующие равенства:*

$$P_{im}^l = \left(\frac{2}{s}\right)^l, \quad P_{podm}^l(t) = \left(\frac{1}{s-1}\right)^t.$$

Доказательство следует из предложения 2 и работы [5].

Вернемся к ортогональным таблицам. Пусть имеется разбиение (3) с условием (4). Пусть также для чисел s и n существует ортогональная таблица $OA(s, n)$ над множеством $V = \{v_1, ..., v_s\}$, $1 < n < s$. Построим из данной таблицы (как и до теоремы 2) матрицу A размера $(s^2-s)\times n$. А на основе матрицы A, как и ранее, построим матрицу зашифрования B размера $r \times 2$ для опорного шифра.

Предложение 5. *Полученный шифр Σ_H будет являться совершенным, причем будут выполнены следующие равенства:*

$$P_{im}^l = \left(\frac{n}{s}\right)^l, \quad P_{podm}^l(t) = \left(\frac{n-1}{s-1}\right)^t.$$

Доказательство следует из теоремы 2 и предложения 2.

Литература

1. Холл, М. Комбинаторика: пер. с англ. / М. Холл. – М.: Мир, 1970. – 212 с.
2. Bose, R.S. On the Applications of the Properties of Galois Fields to the Problems of Construction of Hyper-Graeco-Latin Squares / R.S. Bose // Indian J. Stat. – 1938. – V. 4, №. 3. – P. 323–338.
3. Зубов, А.Ю. Криптографические методы защиты информации. Совершенные шифры / А.Ю. Зубов. – М.: Гелиос АРВ, 2005. – 192 с.
4. Рацеев, С.М. О совершенных имитостойких шифрах / С.М. Рацеев // Прикладная дискретная математика. – 2012. – Т. 17, № 3. – С. 41–47.
5. Рацеев, С.М. О совершенных имитостойких шифрах замены с неограниченным ключом / С.М. Рацеев // Вестник Самарского государственного университета. Естественнонаучная серия. – 2013. – Т. 110, № 9/1. – С. 42–48.
6. Рацеев, С.М. Об оптимальных кодах аутентификации / С.М. Рацеев // Системы и средства информатики. – 2013. Т. 23, № 1. – С. 53–57.

Сергей Михайлович Рацеев, кандидат физико-математических наук, доцент, кафедра «Информационная безопасность и теория управления», Ульяновский государственный университет (г. Ульяновск, Российская Федерация), RatseevSM@mail.ru.

Ольга Ивановна Череватенко, кандидат физико-математических наук, доцент, кафедра «Высшая математика», Ульяновский государственный педагогический университет имени И.Н. Ульянова (г. Ульяновск, Российская Федерация), chai@pisem.net.

Поступила в редакцию 24 января 2014 г.

Bulletin of the South Ural State University.
Series "Mathematical Modelling, Programming & Computer Software",
2014, vol. 7, no. 2, pp. 66–73.

MSC 68P25, 94A60 **DOI: 10.14529/mmp140206**

On Perfect Ciphers Based on Orthogonal Tables

S.M. Ratseev, Ulyanovsk State University, Ulyanovsk, Russian Federation, RatseevSM@mail.ru**,**
O.I. Cherevatenko, Ulyanovsk State I.N. Ulyanov Pedagogical University, Ulyanovsk, Russian Federation, chai@pisem.net

We study perfect imitation resistant ciphers, highlighting particularly the case in which the probabilities of successful imitation and substitution attain their lower limits. It is known that the Vernam cipher with equiprobable gamma is a perfect cipher, but it is maximally vulnerable to imitation attempts owing to its use of alphabets of the same size for plaintexts and ciphertexts. Since the limitation on the size of the sets of plaintexts and keys is a drawback of the mathematical model of the cipher, we begin by studying Zubov's mathematical model of substitution cipher with unbounded key. Basing on this model, we construct models of perfect imitation resistant ciphers. These ciphers use orthogonal tables and Latin rectangles. We study the case in which the generator of random key sequences need not have the uniform probability distribution. Since the keys of these ciphers are at least as long as the transmitted messages, substitution ciphers with unbounded key should be used in very important cases.

Keywords: cipher; perfect cipher; imitation of message.

References

1. Holl M. *Combinatorics*. Waltham (Massachusetts), Blaisdell Publishing, 1967. 310 p.
2. Bose R.S. On the Applications of the Properties of Galois Fields to the Problems of Construction of Hyper-Graeco-Latin Square. *Indian J. Stat*, 1938, vol. 4, issue 3, pp. 323–338.
3. Zubov A.Yu. *Kriptograficheskie metody zashhity informacii. Sovershennye shifry* [Cryptographic Methods of Information Security. Perfect Ciphers]. Moscow, Gelios ARV, 2005. 192 p.
4. Ratseev S.M. [On Perfect Imitation Resistant Ciphers]. *Prikladnaya Diskretnaya Matematika* [Applied Discrete Mathematics], 2012, vol. 17, issue 3, pp. 41–47. (in Russian)
5. Ratseev S.M. [On Perfect Imitation Resistant Ciphers with Unbounded Key]. *Vestnik Samarskogo Gosudarstvennogo Universiteta. Estestvennonauchnaya seriya* [Vestnik of Samara State University. Natural Science Series], 2013, vol. 110, issue 9/1, pp. 45–50. (in Russian)
6. Ratseev S.M. [On optimal Authentication Code]. *Sistemy i Sredstva Informatiki* [Systems and Means of Informatics], 2013, vol. 23, issue 1, pp. 53–57. (in Russian)

Received January 24, 2014