Лекция 1. Введение. Примеры шифров.

Цель лекции: дать основные понятия дисциплины, ее цели и задачи.

План лекции:
Введение.
1 Определение шифра, простейшие примеры.
Заключение
Контрольные вопросы

Ключевые слова: [выбрать самостоятельно].

Содержание лекции:

Введение

Защита информации опирается на набор механизмов и методов, которые, будучи разумно использованы, позволяют гарантировать невозможность атак противника на защищаемую информацию. Криптоалгоритмы являются существенной частью этого набора. Криптоалгоритмы – это алгоритмы преобразования данных, использующие «секрет». Основной параметр качества криптоалгоритма – устойчивость к попыткам противника открыть «секрет». Такая устойчивость в криптографии называется стойкостью.

Криптографическую стойкость надо обосновывать, так как в защите критической информации логика: «я не могу раскрыть «секрет», следовательно, никто не может» неприменима. Методы обоснования криптографической стойкости основаны на накопленном опыте раскрытия «секретов» криптоалгоритмов. Этот опыт сформулирован в методах анализа шифров (один из классов криптоалгоритмов), т.е. в найденных методах и подходах в раскрытии «секретов». Могут найтись гении, придумавшие новые методы анализа, тогда надо пересмотреть стойкость уже используемых криптоалгоритмов или опереться на вновь найденные методы при синтезе новых криптоалгоритмов. Кроме стойкости криптоалгоритмы должны удовлетворять ряду других требований, например, экономичности, скорости реализации и т.п. Совокупность подходов, позволяющих удовлетворить заданному набору требований, составляет теорию синтеза криптоалгоритмов. Методы анализа и синтеза основаны на математике. В основном нужды анализа и синтеза криптоалгоритмов обслуживают дискретная математика, алгебра и теория вероятностей. Более того, криптография дала развитие многим направлениям математики. Изучение вопросов анализа и синтеза начнем с описания простейших шифров.

В соответствии с традицией современной криптографии курс лекций содержит описание наиболее известных универсальных методов криптоанализа, методов анализа блочных и поточных шифров, методов анализа хэш-функций и алгоритмов с несимметричным ключом. По мере знакомства с методами анализа бумем рассматривать и материал, содержащий методы синтеза криптоалгоритмов.

1 Определение шифра, простейшие примеры.

Пусть даны конечные множества X, Y, K. Будем интерпретировать элементы X как открытые сообщения, элементы Y как шифрованные тексты, элементы K – как ключи.
Определение 1. Отображение $T: X \times K \to Y$ *называется шифром, если для* $\forall k \in K \; \exists \, T^{-1}(y, k) = x$.

Пример 1. Пусть $A = \{a_1, \ldots, a_m\}$ – конечный алфавит, S_m – множество всех подстановок на A. Для некоторого натурального n проложим $X = A^n$. Если $x = (a_{i_1}, \ldots, a_{i_n})$, $k \in S_m$, то определим шифр простой замены следующим образом:

$$T(x, k) = \left(k(a_{i_1}), k(a_{i_2}), \ldots, k(a_{i_n})\right)$$

Так как в группе Sm для каждого элемента k есть обратный k^{-1} так, что $k \cdot k^{-1} = e$ – тождественная подстановка, то

$$T^{-1}\left(\left(k(a_{i_1}), k(a_{i_2}), \dots, k(a_{i_n})\right), k\right) = \left(k^{-1}k(a_{i_1}), k^{-1}k(a_{i_2}), \dots, k^{-1}k(a_{i_n})\right) = \\ = (a_{i_1}, \dots, a_{i_n}) = x$$

Таким образом, мы доказали, что для $\forall\ n$ шифр простой замены действительно удовлетворяет определению шифра.

Пример 2. Пусть A = {a_1, ..., a_m} – конечный алфавит, n – натуральное, S_n – симметричная группа подстановок на множестве {1, ..., n}, $X = A^n$. Если

$$x = (a_{i_1}, \dots, a_{i_n}), \quad k = \begin{pmatrix} 1 & \dots & n \\ j_1 & \dots & j_n \end{pmatrix} \in S_n,$$

то шифр перестановки на X определяется следующим образом:

$$T(x, k) = \left(a_{i_{j_1}}, a_{i_{j_2}}, \dots, a_{i_{j_n}}\right).$$

Если $k^{-1}(j_1, \dots, j_n)$ – обратная к k подстановка в S_n, то

$$T^{-1}\left(\left(a_{i_{j_1}}, a_{i_{j_2}}, \dots, a_{i_{j_n}}\right), k\right) = (a_{i_1}, \dots, a_{i_n}).$$

Тем самым также доказано, что шифр перестановки удовлетворяет определению шифра.

Пример 3. В отечественной криптографии следующий шифр Вернама [[1], с. 346] получил название гаммирование. Пусть A = {0, ..., m – 1} – алфавит, $X = A^n$ – множество открытых текстов. Рассмотрим кольцо вычетов Z/m. Положим $K = A^n$ и для $\forall x \in X, k \in K$ определим преобразование

$$y = T(x, k) = x + k,$$

где «+» – сложение по mod m, т.е. сложение в Z/m (соответственно обратная операция обозначается «–»). Введенное преобразование – шифр, т.к. для любого фиксированного k существует обратное отображение

$$T^{-1}(y, k) = y - k = x.$$

Традиционно для данного вида шифра ключ K обозначается греческой буквой γ, откуда в отечественной криптографии и появилось соответствующее название. Так как гамму при больших n часто записывали в блокнот, то за рубежом используется термин блокнотный шифр (pad).

Пример 4. Американский стандарт шифрования, известный под названием DES [[2], с. 250]. Этот шифр реализует простую замену на алфавите из всех двоичных векторов длины 64 бита. Выбор подстановки осуществляется по ключу длиной 56 бит. Ключ преобразуется в 16 48-битовых комбинаций. Подстановки вычисляются для любого 64-битного вектора открытого текста путем реализации 16 циклов повторения одного преобразования. На вход i-го преобразования поступают два 32-битных (левый L_{i-1}, правый – R_{i-1}) вектора, полученных от предыдущего цикла или это входной вектор, переставленный по

---

[1] Шеннон К. Работы по теории информации и кибернетике, М.: Иностранная литература, 1963.

[2] Хоффман Л. Дж. Современные методы защиты информации, М.: Сов. Радио, 1980.

перестановке IP, и разделенный пополам на две 32-битных части (левую L_0 и правую R_0). Еще одним входом для i-го цикла преобразования является 48-битная комбинация ключа. Результатом i-го цикла преобразования является составленный из двух 32-битных частей (левой L_i и правой R_i) 64-битный вектор промежуточного шифртекста. Схема DES условно представлена на рисунке 1. На этой схеме $\oplus$ – побитовое сложение двух 32-битных векторов по модулю 2, IP – перестановка бит, IP^{-1} обратная к IP перестановка. Перестановки IP и IP^{-1} представлены в таблице 1.

Таблица 1. Начальная и обратная перестановки DES.

IP									IP^{-1}							
58	50	42	34	26	18	10	2		40	8	48	16	56	24	64	32
60	52	44	36	28	20	12	4		39	7	47	15	55	23	63	31
62	54	46	38	30	22	14	6		38	6	46	14	54	22	62	30
64	56	48	40	32	24	16	8		37	5	45	13	53	21	61	29
57	49	41	33	25	17	9	1		36	4	44	12	52	20	60	28
59	51	43	35	27	19	11	3		35	3	43	11	51	19	59	27
61	53	45	37	29	21	13	5		34	2	42	10	50	18	58	26
63	55	47	39	31	23	15	7		33	1	41	9	49	17	57	25

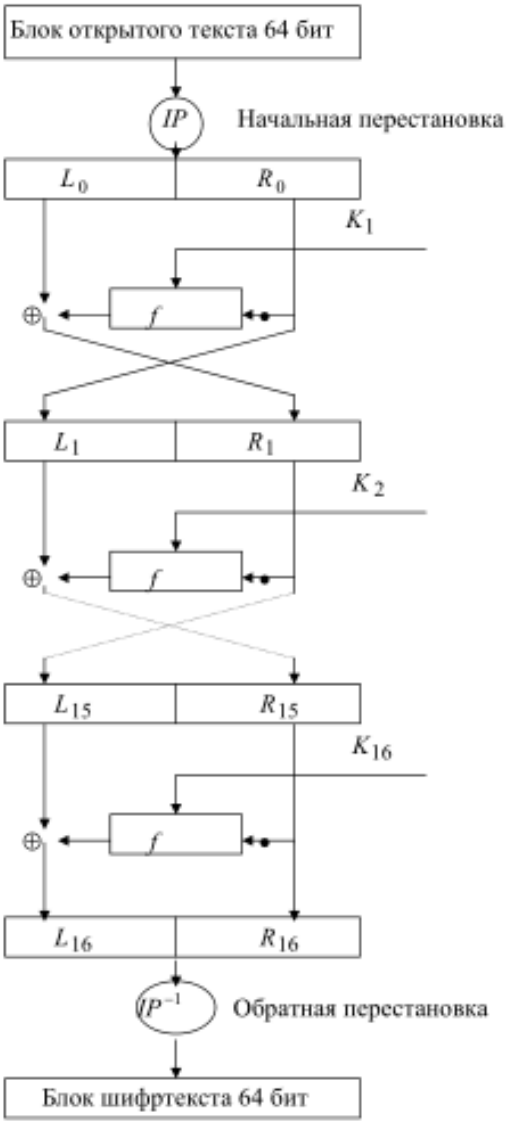

Рис. 1. Схема алгоритма DES

Алгоритм вычисления функции f представлен на рисунке 2.

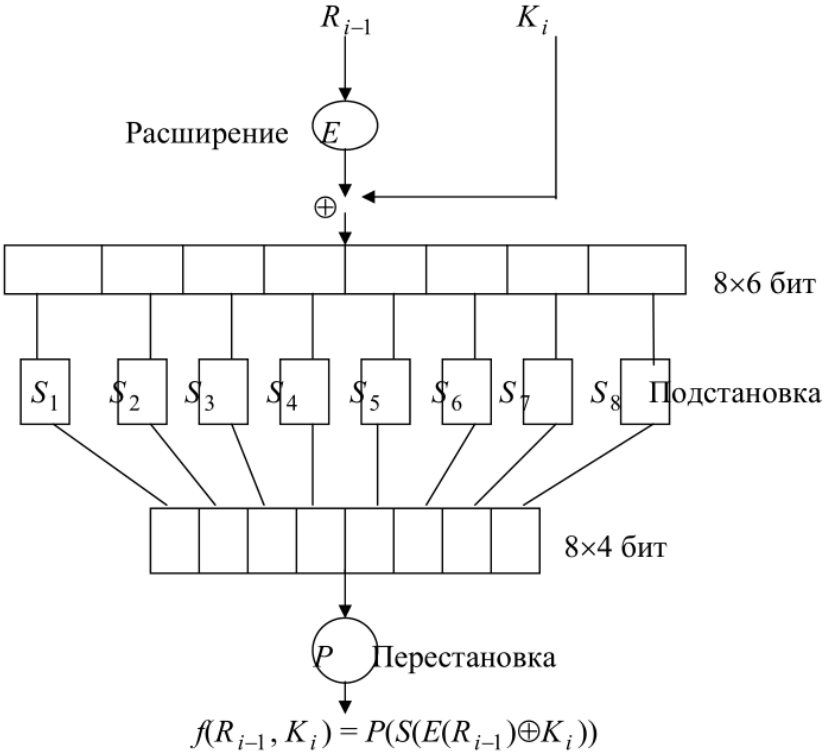

Рис. 2. Схема функции усложнения DES

Таблица 2. Функция расширения и перестановка в функции f усложнения DES.

E							P			
32	1	2	3	4	5		16	7	20	21
4	5	6	7	8	9		29	12	28	17
8	9	10	11	12	13		1	15	23	26
12	13	14	15	16	17		5	18	31	10
16	17	18	19	20	21		2	8	24	14
20	21	22	23	24	25		32	27	3	9
24	25	26	27	28	29		19	13	30	6
28	29	30	31	32	1		22	11	4	25

Схема S_i бокса представлена на рисунке 3. S боксы DES приведены в таблице 3. Здесь контрольные биты CL и CR являются входами в таблицу по горизонтали, а 1 – 4 биты – входами в таблицу по горизонтали. Так, например, $S_1(1, 0, 1, 1, 1, 0) = (1, 0, 1, 1)$.

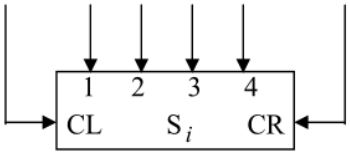

Рис. 3. Схема S-бокса DES. Здесь CL – левый контрольный бит, CR – правый контрольный бит

Таблица 3. S боксы DES.

S_1																	
CL	**CR**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
0	**0**	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7

0	**1**	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
1	**0**	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
1	**1**	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

S_2

CL	**CR**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
0	**0**	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
0	**1**	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	2
1	**0**	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
1	**1**	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

S_3

CL	**CR**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
0	**0**	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
0	**1**	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
1	**0**	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
1	**1**	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

S_4

CL	**CR**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
0	**0**	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
0	**1**	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
1	**0**	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
1	**1**	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

S_5

CL	**CR**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
0	**0**	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
0	**1**	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
1	**0**	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
1	**1**	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

S_6

CL	**CR**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
0	**0**	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
0	**1**	10	12	4	2	7	12	9	5	6	1	13	14	0	11	3	8
1	**0**	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
1	**1**	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

S_7

CL	**CR**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
0	**0**	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
0	**1**	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
1	**0**	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
1	**1**	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

S_8

CL	**CR**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
0	**0**	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
0	**1**	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
1	**0**	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
1	**1**	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Ключи K_l, …, K_{16} получаются из 64 бит ключа DES следующим образом. Определим v_i, $1 \le i \le 16$ следующим образом: $v_i = 1$ для $i = \{1, 2, 9, 16\}$ и $v_i = 2$ для остальных i. Из 64 бит ключа выбираются 56 бит и делятся на две части C_0 и D_0 по 28 бит согласно PC1 в таблице 4. C_0 и D_0 записываются в два циклических регистра сдвига влево. На каждом цикле оба регистра сдвигаются на v_i, $1 \le i \le 16$, бит, получая таким образом C_i и D_i. В сумме

получается сдвиг на 28 бит, что возвращает заполнения регистров в исходное положение. Ключ K_i, $1 \le i \le 16$, получается из C_i и D_i согласно PC2 в таблице 4.

Таблица 4.

PC1													
C_i							**D_i**						
57	49	41	33	25	17	9	63	55	47	39	31	23	15
1	58	50	42	34	26	18	7	62	54	46	38	30	22
10	2	59	51	43	35	27	14	6	61	53	45	37	29
19	11	3	60	52	44	36	21	13	5	28	20	12	4

PC2					
14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

При любом данном k расшифрование DES отличается от зашифрования только тем, что регистры сдвигаются вправо в порядке, обратном зашифрованию. Начинается расшифрование с перестановки бит IP^{-1}, а заканчивается перестановкой IP. DES сыграл в США огромную роль при формировании системы электронных платежей. В настоящее время известно более 65 официальных производителей реализаций DES в виде программного обеспечения или микросхем.

Пример 5. Российский стандарт шифрования ГОСТ 28147-89 [[3], с. 331]. Рассмотрим режим простой замены ГОСТ 28147-89.Этот режим является основным и на его основе реализуются другие режимы шифрования.

Исходный открытый текст M (бинарная последовательность) разбивается на блоки длиной 64 бит:

$$M = M_1M_2 \dots M_t\ ,\ |M_i| = 64.$$

Длина ключа K равна 256 битам. Ключ K разбивается на блоки длиной 32 бит:

$$K = P_1P_2 \dots P_8\ ,\ |P_i| = 32,\ i = 1, \dots, 8.$$

При шифровании используется ключевая последовательность:

$$(K_1, K_2, \dots, K_{31}, K_{32}) = (P_1, P_2, \dots, P_8,\quad P_1, P_2, \dots, P_8,\quad \dots,\quad P_1, P_2, \dots, P_8,\quad P_8, P_7, \dots, P_1),$$

а при расшифровании используется ключевая последовательность:

$$(K_1', K_2', \dots, K_{31}', K_{32}')=(P_1, \dots, P_7, P_8,\quad P_8, P_7, \dots, P_1,\quad \dots,\quad P_8, P_7, \dots, P_1,\quad P_8, P_7, \dots, P_1),$$

Таким образом,

$$K_i' = K_{n+1-i},\quad i = 1, 2, \dots, n;\quad n = 32.$$

[3] Schneier B. Applied Cryptography Second Edition: protocols, algorithms and source code in C. John Wiley & Sons Inc., 1996.

Функция сдвига R определяется следующим образом:

$$R(\alpha_1\alpha_2\ldots\alpha_{32}) = \alpha_{12}\alpha_{13}\ldots\alpha_{32}\alpha_1\alpha_2\ldots\alpha_{11}.$$

Обозначим через «+» сложение по модулю 2^{32} ; $\oplus$ – побитное сложение (исключающее ИЛИ); «+'» – сложение по модулю $2^{32} - 1$.

Блок подстановки реализует функцию:

$$f_s(w), \quad |w| = 32.$$

Функция $f_s(w)$ – это подстановка на множестве $\{0, 1\}^{32}$. Параметр S является сменным и определяет долговременные ключи криптосистемы ГОСТ 28147-89. Подстановка S задается в виде последовательности $S = (\pi_1, \pi_2, \ldots, \pi_8)$, где π_i – подстановка на множестве Ω = {0, 1, 2, ..., 9, A, B, C, D, E, F} (множество всех цифр 16-ричной системы счисления). Каждый элемент из Ω естественным образом отождествляем с соответствующим четырехразрядным двоичным числом (последовательностью из четырех бит). Из определения S следует, что число различных выборов этого параметра равно $(16!)^8$. Значение функции $f_s(w)$ вычисляется следующим образом. Если $w = v_1v_2...v_8$, $|v_i| = 4$, то

$$f_s(w) = \pi_1(v_1)\pi_2(v_2) \ldots \pi_8(v_8).$$

Процедура зашифрования выглядит следующим образом. Пусть $M = \alpha_1\alpha_2\ldots\alpha_{64}$ – блок открытого текста. Введем обозначения:

$$a_0 = \alpha_{32}\alpha_{31}\ldots\alpha_1, \quad b_0 = \alpha_{64}\alpha_{63}\ldots\alpha_{33}.$$

Тогда, процедура зашифрования блока M при помощи криптоалгоритма ГОСТ 28147-89 описывается следующим рекурсивными уравнениями:

$$\begin{aligned} x_i &= a_{i-1} + k_i, \\ y_i &= f_S(x_i), \\ z_i &= R(y_i), \\ a_i &= Z_i \oplus b_{i-1}, \\ b_i &= a_{i-1}, \end{aligned} \qquad (1)$$

i = 1, …, n – 1; n = 32.

$$\begin{aligned} x_n &= a_{n-1} + k_n, \\ y_n &= f_S(x_n), \\ z_n &= R(y_n), \\ a_n &= a_{n-1}, \\ b_n &= z_n \oplus b_{n-1}. \end{aligned} \qquad (2)$$

Если $a_n = \beta_1, \beta_2, \ldots, \beta_{32}$, $b_n = \gamma_1, \gamma_2, \ldots, \gamma_{32}$ и T – блок шифрованного текста, соответствующий блоку открытого текста M, то

$$T = \text{ГОСТ}_K(M) = \beta_{32}\ldots\beta_1\gamma_{32}\ldots\gamma_1.$$

Убедимся, что $\text{ГОСТ}_{K'}(T) = M$, где $T = \text{ГОСТ}_K(M) = \beta_{32}...\beta_1\gamma_{32}...\gamma_1$, $a_n = \beta_1...\beta_{32}$, $b_n = \gamma_1...\gamma_{32}$, $K' = K_nK_{n-1} \ldots K_1$, т.е. $K'_i = K_{n+1-i}$, i = 1, ..., n.

Из сказанного выше следует, что

$$a'_0 = a_n, \qquad b'_0 = b_n.$$

И при i = 1, из системы (1) получим:

$$x'_1 = a'_0 + k'_1 = a_n + k_n.$$

Поскольку, согласно (2), $a_n = a_{n-1}$, то

$$x'_1 = a_{n-1} + k_n = x_n.$$

Поэтому, учитывая (1) и (2) будем иметь:

$$y'_1 = f_S(x'_1) = y_n,$$
$$z'_1 = R(y'_1) = R(y_n) = z_n,$$
$$a'_1 = z'_1 \oplus b'_0 = z_n \oplus b_n = z_n \oplus (z_n \oplus b_{n-1}) = b_{n-1},$$
$$b'_1 = a'_0 = a_n = a_{n-1}.$$

Допустим, что мы уже установили справедливость соотношений

$$a'_{i-1} = b_{n-i+1}, \quad b'_{i-1} = a_{n-i+1}, \tag{3}$$

при всех $k \le i - 1$, $i \ge 2$. Докажем их справедливость для к = i. Согласно алгоритму зашифрования и индуктивному предположению (3), из (1) следует, что

$$x'_i = a'_{i-1} + k'_i = b_{n+1-i} + k_{n+1-i} = a_{n+i} + k_{n+1-i} = x_{n+1-i}.$$

Следовательно,

$$y'_i = f_S(x_{n+1-i}) = y_{n+1-i},$$
$$z'_i = R(y_{n+1-i}) = z_{n+1-i},$$
$$a'_i = z'_i \oplus b'_{i-1} = z_{n+1-i} \oplus a_{n+1-i} = z_{n+1-i} \oplus (z_{n+1-i} \oplus b_{n-i}) = b_{n-i},$$
$$b'_i = a'_{i-1} = b_{n+1-i} = a_{n-i}.$$

Таким образом, для любого i = 1, ..., n

$$a'_i = b_{n-i}, \quad b'_i = a_{n-i}.$$

В частности, $a'_{n-1} = b_1$, $b'_{n-1} = a_1$. Поэтому из (1) и (2) будем иметь:

$$x'_n = a'_{n-1} + k'_n = b_1 + k_1 = a_0 + k_1 = x_1,$$
$$y'_n = f_{s'}(x_1) = y_1; \quad z'_n = R(y_1) = z_1,$$
$$a'_n = a'_{n-1} = b_1,$$
$$b'_n = z'_n \oplus b'_{n-1} = z_1 \oplus a_1 \oplus z_1 \oplus (z_1 \oplus b_0) = b_0.$$

Следовательно, $T' = \text{ГОСТ}_K(T) = M$ и взаимная однозначность криптографического преобразования ГОСТ 28147-89 установлена.

Заключение

Контрольные вопросы

Смотри руководство по организации самостоятельной работы магистрантов.