ГОСТ 28147-89

Стандарт криптографической защиты данных (СКЗД), принятый в СССР в 1989 году, предусматривает шифрование 64-битовых блоков открытых данных под управлением 256-битового секретного ключа, представленного в виде массива из восьми 32-битовых подключей $K = (k_0, k_1, \ldots, k_7)$. ГОСТ 28147-89 определяет три режима шифрования данных (простая замена, гаммирование и гаммирование с обратной связью) и режим выработки имитовставки.

1. *Режим простой замены* (режим электронной кодовой книги). Процедура шифрования соответствует итеративной схеме Фейстеля (см. рис. 1), в которой раундовая функция $F(\mathrm{R}, k)$ задается операциями побитового сложения по модулю 2 ($\oplus$), арифметического сложения по модулю 2^{32} ($\boxplus$) и циклического сдвига влево на 11 битов (rol_{11}), выполняемыми над 32-битовыми подблоками (словами), а также табличными подстановками. Число раундов шифрования равно 32.

Табличные подстановки над 32-битовым блоком V выполняются следующим образом. Блок V разбивается на восемь полубайтов (4-битовых подблоков): $V = v_7 \| v_6 \| v_5 \| v_4 \| v_3 \| v_2 \| v_1 \| v_0$. Для каждого полубайта v_i выполняется операция подстановки (замены), задаваемая таблицей S_i, $i = 0, 1, \ldots, 7$. Каждая из таблиц S_i (их называют -блоками) представляет собой перестановку чисел (полубайтов) 0, 1,..., 15. В результате операции подстановки блок V заменяется на блок

$S(V) = S_7(v_7) \| S_6(v_6) \| S_5(v_5) \| S_4(v_4) \| S_3(v_3) \| S_2(v_2) \| S_1(v_1) \| S_0(v_0)$,

где $S_i(v_i)$ – результат замены v_i на соответствующее значение с использованием таблицы S_i, $i = 0, 1, \ldots, 7$. Например, если $S_1 = (10,7,0,8,14,3,6,13,5,2,9,4,11,15,12)$, то $S_1(0000) = 1010$, $S_1(0001) = 0111, \ldots, S_1(1111) = 1100$.

ГОСТ 28147-89 не определяет способ задания -блоков. Их можно считать секретными элементами, что является дополнительным секретным ключом. Набор -блоков, приведенный в табл.1, рекомендован уже позднее ГОСТом Р 34.11-9 (см. Приложение 1).

Таблица 1

S-блоки ГОСТ 28147-89

v_i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
S_0	4	10	9	2	13	8	0	14	6	11	1	12	7	15	5	3
S_1	14	11	4	12	6	13	15	10	2	3	8	1	0	7	5	9
S_2	5	8	1	13	10	3	4	2	14	15	12	7	6	0	9	11
S_3	7	13	10	1	0	8	9	15	14	4	6	12	11	2	5	3
S_4	6	12	7	1	5	15	13	8	4	10	9	14	0	3	11	2
S_5	4	11	10	0	7	2	1	13	3	6	8	5	9	12	15	14
S_6	13	11	4	1	3	15	5	9	0	10	14	7	6	8	2	12
S_7	1	15	13	0	5	7	10	4	9	2	3	14	6	11	8	12

Функция $F(R,q)$, аргументами и значением которой являются 32-битовые блоки, определяется как

$$V := R \boxplus q;\ V := S(V);\ F := rol_{11}(V).$$

Алгоритм зашифрования

Вход: $\mathrm{D} = (\mathrm{L}, \mathrm{R})$ – 64-битовый блок открытых данных, разбитый на левую и правую половины L и R.

for $i := 0$ ***to*** 30 ***do*** {

if $i \le 23$ ***then*** $j := i \bmod 8$ ***else*** $j := 31 - i$;

$V := R$;

$R := L \oplus F(R, k_j)$;

$L := V$

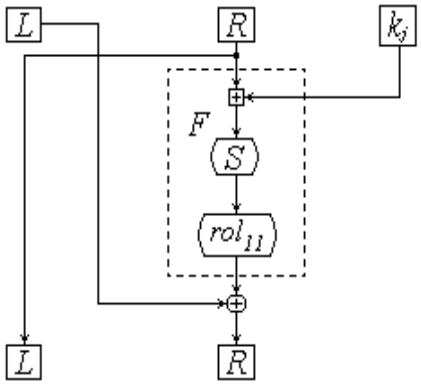
};

$L := L \oplus F(R, k_0)$.

Выход: $C = (L, R)$ – 64-битовый блок шифртекста.

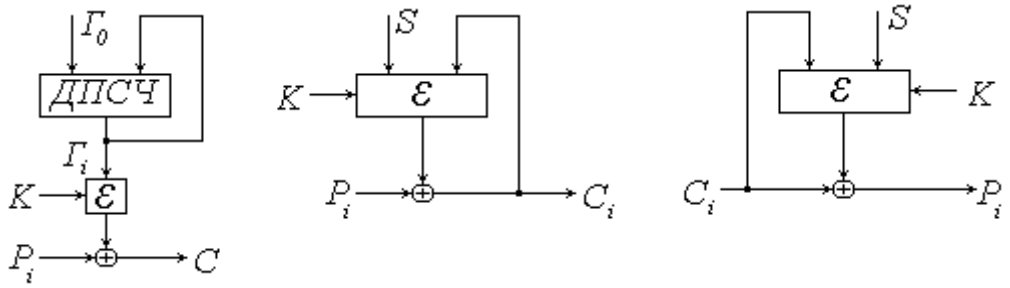
Расшифрование выполняется точно так же, как и зашифрование. Единственное отличие состоит в том, что ключи k_j используются в обратном порядке:

$$\boldsymbol{if}\ i \le 7\ \boldsymbol{then}\ j := i\ \boldsymbol{else}\ j := 7 - (i\ mod\ 8)\,.$$



$\{V := R;\ R := L \oplus rol_{11}(S(R + k_j));\ L := V\}$.

Рис. 1. *Один цикл преобразования* ГОСТ $28147 - 89$



а) *б*) *в*)

Рис. 2. *а*) *Зашифрование в режиме гаммирования. Расшифрование осуществляется по той же схеме.* ДПСЧ *– датчик псевдослучайных чисел, используемых для выработки гаммы. б*) *Зашифрование и в*) *расшифрование в режиме гаммирования с обратной связью.*

2. ***Режим гаммирования.*** Открытый текст P, разбитый на 64-битовые блоки P_1, P_2,..., P_m, преобразуется в шифртекст по правилу:

$$C_i := P_i \oplus \mathcal{E}_k(\Gamma_i), i = 1,2,\ldots,m\,.$$

Другими словами, на текст P накладывается гамма $\mathcal{E}_k(\Gamma_1) \| \mathcal{E}_k(\Gamma_2) \| \ldots \| \mathcal{E}_k(\Gamma_m)$. Здесь $\mathcal{E}_k$ – криптографическое преобразование ГОСТ 28147-89 в режиме простой замены под управлением 256-битового секретного ключа K (см. п. 1). Последовательность 64-битовых псевдослучайных блоков Γ_i, представленных в виде двух 32-битовых подблоков Y_i и Z_i, т.е. $\Gamma_i = (Y_i, Z_i)$, определяется итеративно:

$$Y_i := Y_{i-1} \boxplus const_0;$$

$$Z_i := ((Z_{i-1} + const_1 - 1)\ mod\ (2^{32} - 1)) + 1,$$

где $const_0 = 0x01010101$, $const_1 = 0x01010104$ – 32-битовые константы. Значение $\Gamma_0 = (Y_0, Z_0)$, исходя из которого вычисляются последующие Γ_i, получаются зашифрованием 64-битового блока S, т.е. $\Gamma_0 = \mathcal{E}_k(S)$. Блок S, называемый *синхропосылкой*, передается в от-

крытом виде вместе с зашифрованным сообщением C. Синхропосылка меняется от сообщения к сообщению. Расшифрование осуществляется по той же схеме, что и зашифрование:

$$P_i := C_i \oplus \mathcal{E}_k(\Gamma_i), i = 1,2,\dots,m\,.$$

Процесс шифрования в режиме гаммирования показан на рис. $2a$.

Отметим, что при вычислении Z_i операция сложения по модулю $2^{32}-1$ может быть заменена на сложение по модулю 2^{32}:

$$\mathrm{Z}_i = \begin{cases} \mathrm{Z}_{i-1} \boxplus \mathrm{const}_1, & \text{если } \mathrm{Z}_{i-1} \le (2^{32}-1) - \mathrm{const}_1, \\ \mathrm{Z}_{i-1} \boxplus \mathrm{const}_1 \boxplus 1, & \text{в противном случае,} \end{cases}$$

причем значение $(2^{32}-1) - \mathrm{const}_1$ имеет блок $\mathrm{not}\,\mathrm{const}_1 = \$\mathrm{fefefefe}$.

3. ***Режим гаммирования с обратной связью***. Открытый текст P, разбитый на 64-битовые блоки P_1, P_2,..., P_m, преобразуется в шифртекст $C = C_1, C_2,\dots, C_m$ по правилу:

$\mathrm{C}_1 := P_1 \oplus \mathcal{E}_k(S)$;

$\mathrm{C}_i := P_i \oplus \mathcal{E}_k(C_{i-1}), i = 2,3,..,m,$

где S – 64-битовая синхропосылка (с использованием которой получается первый блок шифртекста), а $\mathcal{E}_k$ – криптографическое преобразование ГОСТ 28147-89 в режиме простой замены под управлением 256-битового секретного ключа K. Расшифрование осуществляется по той же схеме, что и зашифрование. Процесс зашифрования и расшифрования показан на рис. $2б$ и $2в$.

4. ***Режим выработки имитовставки***. В ГОСТ 28147 – 89 подлинность зашифрованных сообщений во всех режимах шифрования может дополнительно подтверждаться с использованием протокола сверки имитовставки.

Имитовставка – это блок I_p из p битов, который вычисляется либо перед зашифрованием, либо параллельно с зашифрованием отдельных блоков. Параметр p $(1 \le p \le 64)$ выбирается в соответствии с установленным уровнем имитозащищенности (с учетом того, что вероятность навязывания ложного сообщения равна $(1/2)^p$).

Пусть $\mathcal{E}_k^{(16)}$ обозначает процедуру зашифрования ГОСТ 28147 – 89 с 16 раундами (вместо стандартных 32 раундов) в режиме простой замены под управлением того же ключа, что и для шифрования данных. Тогда вычисление имитовставки I_p для исходного открытого текста P, разбитого на 64-битовые блоки P_1, P_2,..., P_m (если P_m – неполный блок, то он дополняется нулями), осуществляется по схеме:

$B := \mathcal{E}_k^{(16)}(P_1)$;

$\boldsymbol{for}\ i := 2\ \boldsymbol{to}\ m\ \boldsymbol{do}\ B := \mathcal{E}_k^{(16)}(B \oplus P_i)\,.$

Из 64-битового блока B выбирается p битов (из заранее оговоренных позиций), которые и образуют имитовставку I_p.

Имитовставка присоединяется к шифртексту. Получатель сообщения расшифровывает шифртекст и аналогичным способом вычисляет имитовставку. Если вычисленная получателем имитовставка не совпадает с полученной, то сообщение считается ложным.