Diamond 2

Криптоалгоритм $Diamond\ 2$ [1] шифрует 128-битовые блоки открытых данных под управлением секретного ключа, длина которого может варьироваться от 8 до 65536 битов (стандартное значение − 128 битов). Число R раундов шифрования также не фиксируется, но не меньше 10 (стандартное значение $R = 10$).

$Diamond\ 2$ является SP-сетью, т.е. подстановочно-перестановочным шифром. В алгоритме используются два типа преобразований:

1) фиксированная перестановка битов $P(\mathrm{X})$ в 128-битовом блоке данных X;
2) замена битов в 16-байтовом блоке $\mathrm{X} = (x_0, x_1, \ldots, x_{15})$. Для этого используются $16 \times R$ таблиц замены:

$$S_{1,0},\ S_{1,1},\ldots,S_{1,15}$$
$$\ldots$$
$$S_{R,0},\ S_{R,1},\ldots,S_{R,15}$$

(по 16 таблиц для каждого раунда). Каждая таблица задает подстановку на множестве байтов. Таблицы строятся на этапе предвычислений с использованием датчика псевдослучайных чисел под управлением секретного ключа.

Алгоритм зашифрования

Вход: $X = (x_0, x_1, \ldots, x_{15})$ – 16-байтовый блок открытых данных.

$Y := (S_{1,0}[x_0], S_{1,1}[x_1], \ldots, S_{1,15}[x_{15}])$;
for $i := 2$ ***to*** R ***do*** {
$Z := P(Y)$;
$Y := \left(S_{i,0}[z_0], S_{i,1}[z_1], \ldots, S_{i,15}[z_{15}]\right)$
}.

Выход: Y – 16-байтовый блок шифртекста.

Алгоритм расшифрования

Вход: $Y = (y_0, y_1, \ldots, y_{15})$ – 16-байтовый блок шифртекста.

$X := (S_{R,0}^{-1}[y_0], S_{R,1}^{-1}[y_1], \ldots, S_{R,15}^{-1}[y_{15}])$;
for $i :=$ R ***downto*** 2 ***do*** {
$Z := P^{-1}(X)$;
$X := (\ S_{i,0}^{-1}\ [z_0], S_{i,1}^{-1}\ [z_1], \ldots, S_{i,15}^{-1}\ [z_{15}])$
}.

Выход: X – 16-байтовый блок открытых данных.

Здесь P^{-1} – перестановка, обратная к P; $S_{i,j}^{-1}$ – подстановка, обратная к $S_{i,j}$.

Перестановка P битов в 16-байтовом блоке $X = (x_0, x_1, \ldots, x_{15})$ определяется как

$$P(X) = (y_0, y_1, \ldots, y_{15}),$$

где

$$y_k = \bigvee_{i=0}^{7} \left(x_{i+k} \& 2^i\right), k = 0,1,\ldots,15,$$

а индексы приводятся по модулю 16, т.е. $x_i \equiv x_{i\ mod\ 16}$. Другими словами, k-ый байт результата перестановки формируется из младшего, второго, …, восьмого битов, извлекаемых соответственно из байтов x_k, x_{k+1}, …, x_{k+7}. Обратная перестановка P^{-1} вычисляется аналогично:

$$P^{-1}\ (X) = (y_0, y_1, \ldots, y_{15}),$$

где

$$y_k = \bigvee_{i=0}^{7} \left(x_{k+16-i} \& 2^i\right), k = 0,1,\ldots,15,$$

---

[1] Автор шифра: *Michael Paul Jonson* (США)

Для построения таблиц подстановок $S_{i,j}$ следует либо обратиться к авторской версии, либо разработать собственный способ. Таблицы $S_{i,j}^{-1}$ заполняются следующим образом:

for $i := 1$ ***to*** R ***do***
    for $j := 0$ ***to*** 15 ***do***
        for $x := 0$ ***to*** 255 ***do*** {
            $y \coloneqq S_{i,j}[x]$;
            $S_{i,j}^{-1}[y] \coloneqq x$
        }.