Serpent

Криптоалгоритм $Serpent$ (Змея) [1] шифрует 128-битовые блоки открытых данных под управлением 256-битового секретного ключа. (Допускается использование более короткого ключа – в этом случае он расширяется до требуемого размера добавлением одной битовой единицы и необходимого числа битовых нулей.) Число раундов шифрования равно 32.

$Serpent$ оперирует со 128-битовым блоком данных B, представленным в виде четырех 32-битовых слов: $B = (B_0, B_1, B_2, B_3)$. Биты в словах индексируют от 0 до 31, в 128-битовом блоке – от 0 до 127, а в 256-битовом ключе – от 0 до 255. В словах принят (little-endian-порядок байтов (младший байт размещен слева, занимая младшую адресную позицию).

Алгоритм шифрования представляет собой вариант общей подстановочно-перестановочной сети (SP-сети), построенной по схеме KASLT: "key-addition-substitution-linear transformation″ – прибавление ключевого элемента – подстановка – линейное преобразование. В качестве криптографических операций используются только табличные подстановки и следующие операции над 32-битовыми словами a и b:

$a \oplus b$ – побитовое сложение по модулю 2 слов a и b;

$shl_s(a)$ – сдвиг битов слова a влево на s позиций;

$rol_s(a)$ – циклический сдвиг a влево на s позиций;

(отметим, что $rol_s(a) = shl_s(a) \oplus shl_{32-s}(a) = shl_s(a) \vee shl_{32-s}(a)$, $1 \le s \le 31$).

Таблица 1

Преобразования $L(X)$ и $L^{-1}(X)$ в Serpent

$L(X)$	$L^{-1}(X)$
$X_0 := rol_{13}(X_0);$	$X_2 := rol_{10}(X_2);$
$X_2 := rol_3(X_2);$	$X_0 := rol_{27}(X_0);$
$X_1 := X_1 \oplus X_0 \oplus X_2;$	$X_2 := X_2 \oplus X_3 \oplus shl_7(X_1);$
$X_3 := X_3 \oplus X_2 \oplus shl_3(X_0);$	$X_0 := X_0 \oplus X_1 \oplus X_3;$
$X_1 := rol_1(X_1);$	$X_3 := rol_{25}(X_3);$
$X_3 := rol_7(X_3);$	$X_1 := rol_{31}(X_1);$
$X_0 := X_0 \oplus X_1 \oplus X_3;$	$X_3 := X_3 \oplus X_2 \oplus shl_3(X_0);$
$X_2 := X_2 \oplus X_3 \oplus shl_7(X_1);$	$X_1 := X_1 \oplus X_0 \oplus X_2;$
$X_0 := rol_5(X_0);$	$X_2 := rol_{29}(X_2);$
$X_2 := rol_{22}(X_2).$	$X_0 := rol_{19}(X_0).$

Таблица 2

Таблица замены в $Serpent$ (в 16-ичном представлении)

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
S_0	3	8	f	1	a	6	5	b	e	d	4	2	7	0	9	c
S_1	f	c	2	7	9	0	5	a	1	b	e	8	6	d	3	4
S_2	8	6	7	9	3	c	a	f	d	1	e	4	0	b	5	2
S_3	0	f	b	8	c	9	6	3	d	1	2	4	a	7	5	e
S_4	1	f	8	3	c	0	b	6	2	5	4	a	9	e	7	d
S_5	f	5	2	b	4	a	9	c	0	3	e	8	d	6	7	1
S_6	7	2	c	5	8	4	6	b	e	9	1	f	d	3	a	0
S_7	1	d	f	0	e	8	2	b	7	4	c	a	9	3	5	6

Преобразование L(X) и обратное к нему преобразование $L^{-1}(X)$, определённые в табл. 1, выполняются над 128-битовым блоком $X = (X_0, X_1, X_2, X_3)$, представленным в виде четырех 32-битовых слов X_0, X_1, X_2, X_3.

Табличные подстановки $S_j(x)$, $j = 0, 1, \ldots, 7$, применяются к 128-битовым блокам

[1] Авторы шифра: *Ross Anderson* (Великобритания), *Эли Бихам* (Израиль) и *Lars Knudsen* (Норвегия)

$X = (x_0, x_1,\ldots, x_{31})$, представленным в виде массива из 32 полубайтов (полубайт − четыре бита): каждый из полубайтов x_i заменяется на соответствующий полубайт $S_j(x)$ согласно табл. 2. Например, для блока

$$\mathrm{V} = \quad 15ab503b\ 12436578\ 9af0d84e\ f1e2c3d2$$

имеем:

$$S_3(V) = \quad f9249084\ f8c8693d\ 12e07dc5\ e05ba87b$$

Преобразование $IP(X)$ – это перестановка битов в блоке $X = b_0b_1 \ldots b_{127}$: бит i перемещается в позицию $4(i - 32j) + j$, где $j = i$ div 32, $i = 0, 1,\ldots, 127$. Обратная перестановка $FP(X)$ перемещает бит i в позицию $(i\ div\ 4) + 32(i\ mod\ 4)$, $i = 0, 1,\ldots, 127$.

В алгоритмах зашифрования и расшифрования используются 128-битовые раундовые подключи $K_0, K_1,\ldots, K_{32}$, генерируемые на основе 256-битового секретного ключа K с использованием 32-битовых переменных $W_0, W_1,\ldots, W_{11}$:

$W[0..7] := K;$
$\boldsymbol{for}\ i := 0\ \boldsymbol{to}\ 32\ \boldsymbol{do}\ \{$
$\quad \boldsymbol{for}\ j := 0\ \boldsymbol{to}\ 3\ \boldsymbol{do}\ W_{j+8} := rol_{11}\left(W_j \oplus W_{j+3} \oplus W_{j+5} \oplus W_{j+7} \oplus G \oplus word_4(4i + j)\right);$
$\quad K_i := IP\left(S_{(11-i)mod\ 8}(W[8..11])\right);$
$\quad W[0..7] := W[4..11]$
$\}.$

Здесь $G = 0\text{x}9e3779b9$ – дробная часть отношения золотого сечения $(\sqrt{5} + 1)/2$ в 16-ичном представлении; $word_4(m)$ − 4-байтовое слово со значением m.

Алгоритм зашифрования *Serpent*

Вход: B – 128-битовый блок открытых данных.
$C := IP(B);$
$\boldsymbol{for}\ i := 0\ \boldsymbol{to}\ 30\ \boldsymbol{do}\ C := L(S_{i\ mod\ 8}(C \oplus K_i));$
$C := S_7(C \oplus K_{31}) \oplus K_{32};$
$C := FP(C).$
Выход: C − 128-битовый блок шифртекста .

Алгоритм расшифрования *Serpent*

Вход: C − 128-битовый блок шифртекста.
$B := IP(C);$
$B := S_7^{-1}(B \oplus K_{32}) \oplus K_{31};$
$\boldsymbol{for}\ i := 30\ \boldsymbol{downto}\ 0\ \boldsymbol{do}\ B := S_{i\ mod\ 8}^{-1}(L^{-1}(B)) \oplus K_i;$
$B := FP(B).$
Выход: B − 128-битовый блок открытых данных.