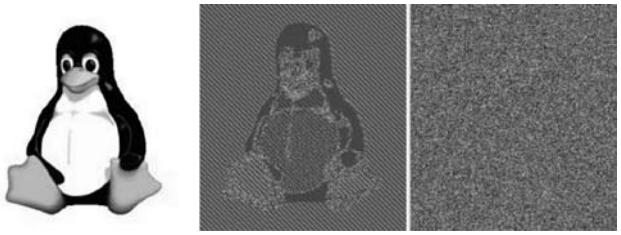
УДК 512.5+519.723

Повышающая криптостойкость оболочка над блоковым шифром Ривеста

А. А. Набебин*, Е. Д. Сапожков

Предложена модификация RC5-S блокового шифра Ривеста RC5, значительно повышающая криптографическую стойкость шифра RC5, в которой использован алгоритм CBC (Cipher Block Chaining) сцепления блоков шифротекста.
Ключевые слова: блоковый шифр, шифрование, дешифрование, криптографическая стойкость, оболочка.

Рассмотрим модификацию RC5-S симметричного блокового шифра RC5 Ривеста, использующую алгоритм CBC (cipher block chaining) сцепления блоков шифротекста [1 — 4]. При работе шифром RC5 одинаковые блоки шифруемого текста преобразуются в одинаковые зашифрованные блоки, что дает криптоаналитикам некую информацию об использованном шифре. При шифровании (рис. 1, *а*) шифр RC5 предлагает шифротекст (рис. 1, *б*) с заметной информацией о характере передаваемого файла. При использовании модификации RC5-S данная информация не предоставляется (рис. 1, *в*). Таким образом, RC5-S можно рассматривать как оболочку над шифром RC5, являющимся составной частью RC5-S.



а *б* *в*

Рис. 1

* anabebin@hse.ru

В блоковом шифре RC5-*w*/*r*/*b* *w* — длина блока; *r* — число раундов (от 0 до 255); *b* — длина ключа в байтах (от 0 до 255). Числа *w*, *r*, *b* могут варьироваться. Обычно рекомендуются шифры RC5-32/12/16, RC5-64/16/16. При этом RC5 может быть реализован аппаратно и программно.

Примем следующие обозначения:

$\boxplus$, $\boxminus$ — сложение и вычитание по модулю $2w$;

$\curvearrowleft$, $\curvearrowright$, *r* — циклические левое и правое вращения на *r* бит;$\curvearrowleft$, $\curvearrowright$,

A — циклические левое и правое вращения на число бит в *A*;

$\oplus$ XOR — бинарное побитовое сложение (по модулю 2).

Генерация ключей в шифре RC5

ВХОД. *b*-байтовый ключ $K = K[0]...K[b-1]$; число раундов *r*; *w*-байтовый блок текста.

ВЫХОД. Расширенные ключи K_0, ..., K_{2r+1}, где K_i — *w*-битовое слово.

1. Генерация констант. Для заданного параметра *w* (с использованием двух математических констант: экспоненты *e* и золотого сечения *f*) генерируются две псевдослучайные величины $Q_w := \text{Odd}((f-1)2^w)$; $P_w := \text{Odd}((e-1)2^w)$, где Odd — округление до ближайшего нечетного целого (таблица).

w	16	32	64
P_w	b7e1	b7e15163	b7e15162 8aed2a6b
Q_w	9e37	9e3779b9	9e3779b9 7f4a7c15

2. Разбиение ключа на слова.

2.1. $u := w/8$ — число байт в слове u; $c = \lceil b/u \rceil$.

2.2. Для i от 0 до $c - 1$ выполнить следующее:

$$L_i := \sum_{j=0}^{u-1} 2^{8 \cdot j} K[iu + j].$$

Для получения числа байт, делящегося на u, т. е. $K[j] := 0$ для $b \le j \le cu - 1$, можно дополнить K справа, при необходимости, нулевыми байтами. Если c не кратен $w/8$, то L_i дополняется справа нулевыми битами до ближайшего большего размера c, кратного $w/8$. Если $b = c = 0$, то устанавливаются значения $c = 1$, $L_0 = 0$.

3. Построение таблицы расширенных ключей.

3.1. $K_0 := P_w$. (P_w взять из таблицы).

3.2. Для i от 1 до $2r + 1$ выполнить следующее:

$$K_i := K_{i-1} \boxplus Q_w \ (Q_w \text{ взять из табл.1}).$$

4. Перемешивание.

4.1. $i := 0$; $j := 0$; $A := 0$; $B := 0$, $t := \max(c, 2r + 2)$.

4.2. Для s от 1 до $3t$:

(a) $K_i := (K_i \boxplus A \boxplus B) \hookleftarrow 3$; $A := K_i$; $i := i + 1 \bmod (2r + 2)$;

(b) $L_j := (L_j \boxplus A \boxplus B) \hookleftarrow (A \boxplus B)$; $B := L_j$; $j := j + 1 \bmod c$.

5. Вернуть K, K_0, K_1, ..., K_{2r+1}.

Алгоритм RE шифрования в RC5 одного блока текста

ВХОД. Поделенный на две половины w-байтовый исходный текст $M = (A, B)$; число раундов — r; ключ $K = K[0] \ldots K[b - 1]$; расширенные ключи $K_0, K_1, \ldots, K_{2r+1}$.

ВЫХОД. w-байтовый шифротекст C.

1. $A := A \boxplus K_0$; $B := B \boxplus K_1$. (Сложение по $\bmod 2^w$).

2. Для i от 1 до r выполнить следующее:

$$A := ((A \oplus B) \hookleftarrow B) \boxplus K_{2i}; \ B := ((B \oplus A) \hookleftarrow A) \boxplus K_{2i+1}.$$

3. $C := (A, B)$.

4. Вернуть шифротекст C.

Алгоритм RD дешифрования в шифре RC5 одного блока шифротекста $C = (A, B)$ работает в порядке, обратном порядку шифрования.

1. Для i from r до 1 выполнить:

$$B := ((B \boxminus K_{2i+1}) \hookrightarrow A) \oplus A; \ A := ((A \boxminus K_{2i}) \hookrightarrow B) \oplus B.$$

2. $M := (A \boxminus K_0, B \boxminus K_1)$.

3. Вернуть M.

Шифр RC5–S

Генерация ключей в RC5-S совпадает с генерацией ключей в RC5.

Шифрование. Исходный битовый текст T делится на блоки длины w байт. Если длина последнего блока меньше w, то дополняем его нулями до длины w и получаем упорядоченное множество $S = \{B_1, B_2, \ldots, B_t\}$ из t блоков.

ВХОД. Ключ K длины b – 1 байт; число раундов — r; длина w блока текста; расширенные ключи $K_0, K_1, \ldots, K_{2r+1}$; множество $S = \{B_1, B_2, \ldots, B_t\}$.

ВЫХОД. Упорядоченное множество $S_1 = \{Y_1, Y_2, \ldots, Y_t\}$ шифрованных блоков.

1. Сгенерировать случайный блок F длины w байт.

2. Сгенерировать случайный инициализирующий вектор V длины w байт.

3. $S_1 := \varnothing$. Записать V в конец S_1 и получить $S_1 = \{V\}$.

4. $G := F \oplus V$ (побайтовый XOR двух блоков).

5. Зашифровать блок G алгоритмом RE и получить блок F_1.

6. Записать F_1 в конец S_1 и получить $S_1 = \{V, F_1\}$.

7. $V_1 := F \oplus F_1$ (побайтовый XOR двух блоков).

8. Для i от 1 до t выполнить следующее:

8.1. $X_i := B_i \oplus V_1$.

8.2. Зашифровать X_i алгоритмом RE и получить Y_i.

8.3. Записать Y_i в конец S_1 и получить

$$S_1 = \{V, S_1, Y_1, Y_2, \ldots, Y_i\}.$$

8.4. $V_1 := Y_i$.

9. Вернуть шифротекст $S_1 = \{V, F_1, Y_1, Y_2, \ldots, Y_t\}$.

Дешифрование.

ВХОД. Шифротекст $S_1 = \{V, F_1, Y_1, Y_2, \ldots, Y_t\}$.

ВЫХОД. $S = \{B_1, B_2, \ldots, B_t\}$.

1. Дешифровать F_1 алгоритмом RD и получить G.

2. $F := G - V = G \oplus V$; $V_1 := F \oplus F_1 = G \oplus V \oplus F_1$; $S := \varnothing$.

3. Для i от 1 до t выполнить следующее.

3.1. Дешифровать Y_i алгоритмом RD и получить X_i.

3.2. $B_i := X_i - V_1 = X_i \oplus V_1$.

3.3. Записать B_t в конец S и получить $S = \{B_1, B_2, \ldots, B_i\}$.

3.4. $V_1 := Y_i$.

4. Вернуть $S = \{B_1, B_2, \ldots, B_t\}$.

Пример. RC5-S-16/16/16. Исходный текст: «Солнце светило ярко, так ярко...» Его 16-ричное представление, состоящее из двух блоков по 16 байт:

D1EEEBEDF6E520F1 E2E5F2E8EBEE20FF
F0EAEE2C20F2E0EA 20FFF0EAEE2E2E2E

Ключ K = 7300610070006F00 7A0068006B006F00

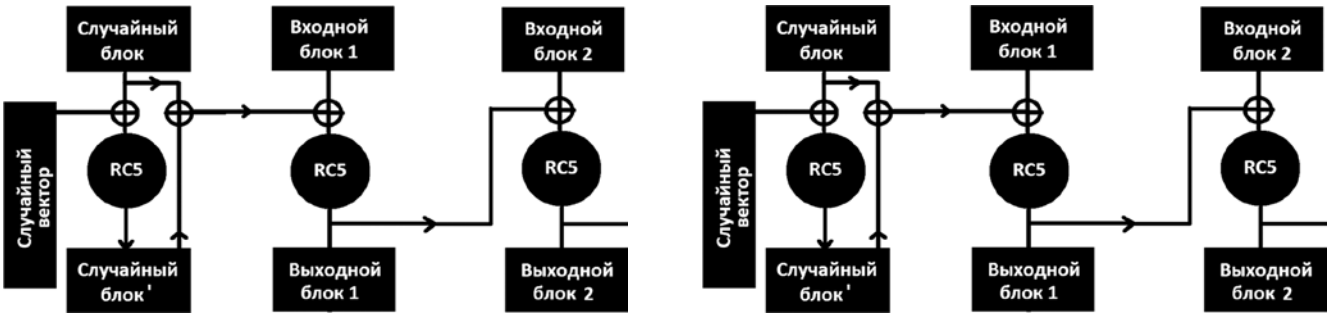
RC5-S при $w = 16$; $r = 16$ и $b = 16$ генерирует шифротекст:

C = 12c32dfd9a31542c b7381a4d99a702a8
2d669719e467cc55 6a16699bb6eb2c6a
a157bb58f62d865a a92625251dd1316d
0240e86fc10c6fca 2d65eefb826ee794,

где первый блок — инициализирующий вектор V; второй блок — F_1, затем следуют два блока шифротекста.

При дешифровании шифротекста RC5-S возвращает исходный текст.

Схемы шифрования и дешифрования показаны на рис. 2 *а*, *б*.



а *б*

Рис. 2.

Литература

1. **Шнайер Б.** Практическая криптография. М.: Триумф, 2002.

2. **Шнайер Б., Фергюсон Н.** Практическая криптография. М.: Вильямс, 2005.

3. **Menezes A., van Oorshot P., Vanstone S.** Handbook of applied cryptography. CRC Press, 1996.

4. **Rivest R.L.** The RC5 encryption algorithm // Proc. second Intern. workshop on fast software encryption (FSE). 1994. P. 86 — 96.

Статья поступила в редакцию 10.07.2015