NUSH

Криптоалгоритм $NUSH$[1] шифрует $4n$-битовые ($n = 16, 32$ или 64) блоки открытых данных под управлением секретного ключа, длина которого может составлять 128, 192 или 256 битов.

Основу алгоритма составляет преобразование R_i, определяемое как

$Ri(a, b, c, d, k, s) \equiv \{$
$\quad c := ror_s((c \oplus k) \boxplus_n b);$
$\quad \textbf{if } (i \bmod 64) \in \{1,3..7,9,10,12,14..17,23,25..27,29,32,33,35,36,38,40,43,44,54,56..58\}$
$\quad \textbf{then } a := a \boxplus_n (c \vee d) \textbf{ else } a := a \boxplus_n (c \& d)$
$\}.$

Здесь a, b, c, d, k – n-битовые слова; $0 \le s \le n - 1$ – целое число; $ror_s x$ – циклический сдвиг слова x вправо на s битов; $\vee$ и $\&$ – побитовые операции дизъюнкции и конъюнкции над n-битовыми словами; $\boxplus_n$ – сложение по модулю 2^n.

Обратное преобразование R_i^{-1} задается как

$R_i^{-1}(a, b, c, d, k, s) \equiv \{$
$\quad \textbf{if } (i \bmod 64) \in \{1,3..7,9,10,12,14..17,23,25..27,29,32,33,35,36,38,40,43,44,54,56..58\}$
$\quad \textbf{then } a := a \boxminus_n (c \vee d) \textbf{ else } a := a \boxminus_n (c \,\&\, d);$
$\quad c := ((ror_{n-s} c) - \boxminus_n b) \oplus k$
$\}.$

Здесь $\boxminus_n$ – вычитание по модулю 2^n.

Алгоритм зашифрования *NUSH*

В алгоритме, состоящем из L итераций (4 итерации $= 1$ раунд) используются n-битовые раундовые подключи $KS[0], \dots, KS[3]$; $KR[0], \dots, KR[L-1]$; $KF[0], \dots, KF[3]$, генерируемые на этапе предвычислений из секретного ключа K, а также n-битовые раундовые константы $C[0], \dots, C[L-1]$ и целые числа $0 \le S[0], \dots, S[L-1] \le n - 1$, заданные таблицей 1. Стандартные значения $L = 36, 68$ и 132 соответственно для $n = 16, 32$ и 64.

Вход: (a, b, c, d) – $4n$-битовый блок открытых данных в виде четырех n-битовых слов a, b, c, d.

$(a, b, c, d) := (a \oplus KS[0], b \oplus KS[1], c \oplus KS[2], d \oplus KS[3]);$
$\textbf{for } i := 0 \textbf{ to } L - 1 \textbf{ do } \{$
$\quad R_i(a, b, c, d, KR[i] \boxplus_n C[i], S[i]);$
$\quad (a, b, c, d) := (b, c, d, a)$
$\};$
$(a, b, c, d) := (a \oplus KF[0], b \oplus KF[1], c \oplus KF[2], d \oplus KF[3])$.

Выход: (a, b, c, d) – 128-битовый блок шифртекста.

Алгоритм расшифрования $NUSH^{-1}$

Вход: (a, b, c, d) – 128-битовый блок шифртекста.

$(a, b, c, d) := (a \oplus KF[0], b \oplus KF[1], c \oplus KF[2], d \oplus KF[3]);$
$\textbf{for } i := L - 1 \textbf{ downto } 0 \textbf{ do } \{$
$\quad (a, b, c, d) := (d, a, b, c)$
$\quad R_i^{-1}(a, b, c, d, KR[i] \boxplus_n C[i], S[i]);$
$\};$
$(a, b, c, d) := (a \oplus KS[0], b \oplus KS[1], c \oplus KS[2], d \oplus KS[3])$.

Выход: (a, b, c, d) – $4n$-битовый блок открытых данных.

---

[1] Авторы шифра: *Лебедев А. Н.* (Компания ЛАН Крипто, Россия), *Волчков А. А.* (Ассоциация РусКрипто, Россия)

Таблица 1.

Константы, используемые в NUSH

1. $n = 16,\ L = 36$
2. $n = 32,\ L = 68$
3. $n = 64,\ L = 132$

Генерация раундовых подключей в *NUSH*

tn-битовый секретный ключ K представляется в виде масива n-битовых слов: $(K[0], K[1], \dots, K[t-1])$.

1. $tn = 128$

$n = 16$			
$KS[0] = K[4]$	$KS[1] = K[5]$	$KS[2] = K[6]$	$KS[3] = K[7]$
$KF[0] = K[3]$	$KF[1] = K[2]$	$KF[2] = K[1]$	$KF[3] = K[0]$
$KR[i] = K[i \bmod 8], i = 0, 1, \dots, 35$			
$n = 32$			
$KS[0] = K[3]$	$KS[1] = K[2]$	$KS[2] = K[1]$	$KS[3] = K[0]$
$KF[0] = K[1]$	$KF[1] = K[0]$	$KF[2] = K[3]$	$KF[3] = K[2]$
$KR[i] = K[i \bmod 4], i = 0, 1, \dots, 67$			
$n = 64$			
$KS[0] = K[1]$	$KS[1] = K[0]$	$KS[2] = K[1]$	$KS[3] = K[0]$
$KF[0] = K[0]$	$KF[1] = K[1]$	$KF[2] = K[0]$	$KF[3] = K[1]$
$KR[i] = K[i \bmod 2], i = 0, 1, \dots, 67$			

2. $tn = 192$

$n = 16$			
$KS[0] = K[4]$	$KS[1] = K[5]$	$KS[2] = K[6]$	$KS[3] = K[7]$
$KF[0] = K[11]$	$KF[10] = K[2]$	$KF[2] = K[9]$	$KF[3] = K[8]$
$KR[i] = K[i \bmod 12], i = 0, 1, \dots, 35$			
$n = 32$			
$KS[0] = K[2]$	$KS[1] = K[3]$	$KS[2] = K[4]$	$KS[3] = K[5]$
$KF[0] = K[5]$	$KF[1] = K[4]$	$KF[2] = K[3]$	$KF[3] = K[2]$
$KR[i] = K[i \bmod 6], i = 0, 1, \dots, 67$			
$n = 64$			
$KS[0] = K[2]$	$KS[1] = K[1]$	$KS[2] = K[0]$	$KS[3] = K[2]$
$KF[0] = K[1]$	$KF[1] = K[2]$	$KF[2] = K[2]$	$KF[3] = K[0]$
$KR[i] = K[i \bmod 3], i = 0, 1, \dots, 67$			

3. $tn = 256$

$n = 16$			
$KS[0] = K[12]$	$KS[1] = K[13]$	$KS[2] = K[14]$	$KS[3] = K[15]$
$KF[0] = K[13]$	$KF[1] = K[12]$	$KF[2] = K[15]$	$KF[3] = K[14]$
$KR[i] = K[i \bmod 16], i = 0, 1, \dots, 35$			
$n = 32$			
$KS[0] = K[4]$	$KS[1] = K[5]$	$KS[2] = K[6]$	$KS[3] = K[7]$
$KF[0] = K[5]$	$KF[1] = K[4]$	$KF[2] = K[7]$	$KF[3] = K[6]$
$KR[i] = K[i \bmod 8], i = 0, 1, \dots, 67$			
$n = 64$			
$KS[0] = K[3]$	$KS[1] = K[2]$	$KS[2] = K[1]$	$KS[3] = K[0]$
$KF[0] = K[2]$	$KF[1] = K[3]$	$KF[2] = K[0]$	$KF[3] = K[1]$
$KR[i] = K[i \bmod 4], i = 0, 1, \dots, 67$			