RC4

Аметов Имиль, гр. M07-903

22 апреля 2020 г.

Задача: Приведите пример работы потокового шифра RC4 для массива размером 16 ячеек и чисел {0...15}.

Решение: Заполняем значения для ячеек состояния S_0, S_1, ..., S_{15}:

S_0	S_1	S_2	S_3	S_4	S_5	S_6	S_7
0	1	2	3	4	5	6	7
S_8	S_9	S_{10}	S_{11}	S_{12}	S_{13}	S_{14}	S_{15}
8	9	10	11	12	13	14	15

Предоставленный по условию ключ выглядит так:

K_0	K_1	K_2	K_3	K_4	K_5	K_6	K_7
0	1	2	3	4	5	6	7
K_8	K_9	K_{10}	K_{11}	K_{12}	K_{13}	K_{14}	K_{15}
8	9	10	11	12	13	14	15

Задаю $j = 0$.

Теперь вычисляется цикл от $i = 0$ до $i = 15$.

Для $i = 0$: $j = (0+S_0+K_0) \mod 16 = (0+0+0) \mod 16 = 0 \mod 16 = 0$. Меняем местами значения для S_0 и S_0.

Для $i = 1$: $j = (0 + 1 + 1) \mod 16 = 2$. Меняем местами S_1 и S_2. В результате $S_1 = 2$ и $S_2 = 1$.

Для $i = 2$: $j = (2 + 1 + 2) \mod 16 = 5$. Меняем местами S_2 и S_5. В результате $S_2 = 5$ и $S_5 = 1$.

Для $i = 3$: $j = (5 + 3 + 3) \mod 16 = 11$. Меняем местами S_3 и S_{11}. В результате $S_3 = 5$ и $S_{11} = 1$.

Для $i = 4$: $j = (11 + 4 + 4) \mod 16 = 3$. Меняем местами S_4 и S_3. В результате $S_4 = 11$ и $S_3 = 4$.

Для $i = 5$: $j = (3 + 1 + 5) \mod 16 = 9$. Меняем местами S_5 и S_9. В результате $S_5 = 9$ и $S_9 = 1$.

Для $i = 6$: $j = (9 + 6 + 6) \mod 16 = 5$. Меняем местами S_6 и S_5. В результате $S_6 = 9$ и $S_5 = 6$.

Для $i = 7$: $j = (5 + 7 + 7) \mod 16 = 3$. Меняем местами S_7 и S_3. В результате $S_7 = 4$ и $S_3 = 7$.

Для $i = 8$: $j = (3 + 8 + 8) \mod 16 = 3$. Меняем местами S_8 и S_3. В результате $S_8 = 7$ и $S_3 = 8$.

Для $i = 9$: $j = (3 + 1 + 9) \mod 16 = 13$. Меняем местами S_9 и S_{13}. В результате $S_9 = 13$ и $S_{13} = 1$.

Для $i = 10$: $j = (13 + 10 + 10) \mod 16 = 1$. Меняем местами S_{10} и S_1. В результате $S_{10} = 2$ и $S_1 = 10$.

Для $i = 11$: $j = (1 + 3 + 11) \mod 16 = 15$. Меняем местами S_{11} и S_{15}. В результате $S_{11} = 15$ и $S_{15} = 3$.

Для $i = 12$: $j = (15 + 12 + 12) \mod 16 = 7$. Меняем местами S_{12} и S_7. В результате $S_{12} = 4$ и $S_7 = 12$.

Для $i = 13$: $j = (7 + 1 + 13) \mod 16 = 5$. Меняем местами S_{13} и S_5. В результате $S_{13} = 6$ и $S_5 = 1$.

Для $i = 14$: $j = (5 + 14 + 14) \mod 16 = 1$. Меняем местами S_{14} и S_1. В результате $S_{14} = 10$ и $S_1 = 14$.

Для $i = 15$: $j = (1 + 3 + 15) \mod 16 = 3$. Меняем местами S_{15} и S_3. В результате $S_{15} = 8$ и $S_3 = 3$.

В итоге таблица состояния имеет вид

S_0	S_1	S_2	S_3	S_4	S_5	S_6	S_7
0	14	5	3	11	1	9	12
S_8	S_9	S_{10}	S_{11}	S_{12}	S_{13}	S_{14}	S_{15}
7	13	2	15	4	6	10	8

Поскольку у меня урезанная версия таблицы состояний, то будет видоизменён алгоритм вычисления следующего байта result (гамма):

1. $i := (i + 1) \mod 16$,
2. $j := (j + S_i) \mod 16$,
3. замена местами S_i и S_j,
4. $t := (S_i + S_j) \mod 16$,
5. result $:= S_t$

Найдём очередную гамму. Вычисляем i: $i = (15 + 1) \mod 16 = 16 \mod 16 = 0$. Вычисляем j: $j = (3 + S_0) \mod 16 = (3 + 0) \mod 16 = 3 \mod 16 = 3$. Меняем местами S_0 и S_3. Получаем, что $S_0 = 3$ и $S_3 = 0$. Вычисляем t: $t = (S_0 + S_3) \mod 16 = (0 + 3) \mod 16 = 3$. И result $= S_3 = 0$.

Шифровка выполняется с помощью операции исключающее-или. В данном случае применение операции исключающего-или не приведёт к шифровке и байт будет передан без преобразования.

Найдём очередную гамму. Вычисляем i: $i = (0 + 1) \mod 16 = 1$. Вычисляем j: $j = (3 + S_1) \mod 16 = (3 + 14) \mod 16 = 1$. Меняем местами S_1 и S_1. Получаем, что $S_1 = 14$ и $S_1 = 14$. Вычисляем t: $t = (S_1 + S_1) \mod 16 = (14 + 14) \mod 16 = 12$. И result $= S_{12} = 4$.

Пусть нужно зашифровать байт со значением 153, в двоичном виде 153 выглядит как 10011001 и гамма 00000100. После применения исключающего-или получим 10011101 в двоичном виде или 157 в десятичном.

Принимающая сторона, в свою очередь применит эту же операцию и получит из 157 исходный байт со значением 153.