GOST

Аметов Имиль, гр. M07-903

4 мая 2020 г.

Задача: Захешировать сообщение

$$M = \begin{matrix} 73\ 65\ 74\ 79 & 62\ 20\ 32\ 33 & 3D\ 68\ 74\ 67 & 6E\ 65\ 6C\ 20 \\ 2C\ 65\ 67\ 61 & 73\ 73\ 65\ 6D & 20\ 73\ 69\ 20 & 73\ 69\ 68\ 54 \end{matrix}$$

Решение: Задаём начальный хеш

$$H = \begin{matrix} 00\ 00\ 00\ 00 & 00\ 00\ 00\ 00 & 00\ 00\ 00\ 00 & 00\ 00\ 00\ 00 \\ 00\ 00\ 00\ 00 & 00\ 00\ 00\ 00 & 00\ 00\ 00\ 00 & 00\ 00\ 00\ 00 \end{matrix}$$

Генерируем ключ K_1, для этого нужно два значения U_1 и V_1. $U_1 = H$ и $V_1 = M$. Получаем

$$U_1 = \begin{matrix} 00\ 00\ 00\ 00 & 00\ 00\ 00\ 00 & 00\ 00\ 00\ 00 & 00\ 00\ 00\ 00 \\ 00\ 00\ 00\ 00 & 00\ 00\ 00\ 00 & 00\ 00\ 00\ 00 & 00\ 00\ 00\ 00 \end{matrix}$$

$$V_1 = \begin{matrix} 73\ 65\ 74\ 79 & 62\ 20\ 32\ 33 & 3D\ 68\ 74\ 67 & 6E\ 65\ 6C\ 20 \\ 2C\ 65\ 67\ 61 & 73\ 73\ 65\ 6D & 20\ 73\ 69\ 20 & 73\ 69\ 68\ 54 \end{matrix}$$

Теперь нужно сложить U_1 и V_1 с помощью операции исключающее-или, также обозначается как $\oplus$. Результат получается таким:

$$U_1 \oplus V_1 = \begin{matrix} 73\ 65\ 74\ 79 & 62\ 20\ 32\ 33 & 3D\ 68\ 74\ 67 & 6E\ 65\ 6C\ 20 \\ 2C\ 65\ 67\ 61 & 73\ 73\ 65\ 6D & 20\ 73\ 69\ 20 & 73\ 69\ 68\ 54 \end{matrix}$$

Для получения K_1 нужно перемешать полученную сумму. Перемешивание производится с помощью Таблицы 1. Здесь s — это номер байта из результата сложения, а $\varphi(s)$ — номер байта в новом массиве, который будет содержать то, что было в байте с номером s в массиве с результатом сложения.

Нумерация s ведётся следующим образом:

1	2	3	4
73	65	74	79
5	6	7	8
2C	65	67	61

То есть, нужно создать новый массив из 32-х байтов и в 1-й байт записать значение 73, в 9-й байт записать 65, в 17-й байт записать 74, в 25-й байт записать 79 и так далее.

В результате получим следующий массив

Таблица 1: Перестановка для s

s	$\varphi(s)$
1	1
2	9
3	17
4	25
5	3
6	11
7	19
8	27
9	5
10	13
11	21
12	29
13	7
14	15
15	23
16	31
17	2
18	10
19	18
20	26
21	4
22	12
23	20
24	28
25	6
26	14
27	22
28	30
29	8
30	16
31	24
32	32

$$K_1 = \begin{array}{cccc} 73\ 3D\ 2C\ 20 & 65\ 68\ 65\ 73 & 74\ 74\ 67\ 69 & 79\ 67\ 61\ 20 \\ 62\ 6E\ 73\ 73 & 20\ 65\ 73\ 69 & 32\ 6C\ 65\ 68 & 33\ 20\ 6D\ 54 \end{array}$$

Вычисление $U_2 = A(U_1) \oplus C_2$.

$$C_2 = \begin{array}{cccc} 00\ 00\ 00\ 00 & 00\ 00\ 00\ 00 & 00\ 00\ 00\ 00 & 00\ 00\ 00\ 00 \\ 00\ 00\ 00\ 00 & 00\ 00\ 00\ 00 & 00\ 00\ 00\ 00 & 00\ 00\ 00\ 00 \end{array}$$

Поэтому

$$U_2 = \begin{array}{cccc} 00\ 00\ 00\ 00 & 00\ 00\ 00\ 00 & 00\ 00\ 00\ 00 & 00\ 00\ 00\ 00 \\ 00\ 00\ 00\ 00 & 00\ 00\ 00\ 00 & 00\ 00\ 00\ 00 & 00\ 00\ 00\ 00 \end{array}$$

Вычисление V_2: $V_2 = A(A(V_1))$. Вычисление $A(X)$ происходит так:

$$A(X) = A(X_4||X_3||X_2||X_1) = (X_1 \oplus X_2)||X_4||X_3||X_2.$$

Как будет вычисляться $A(V_1)$? Здесь $X_1 = 2073692073696854$ и $X_2 = 2C6567617373656D$. Складываем исключающим-или X_1 и X_2 и получаем $X_1 \oplus X_2 = 0C160E41001A0D39$. Полученный результат помещается вместо X_4:

$$V_2 = A(A(V_1)) = \begin{array}{cccc} 0C\ 16\ 0E\ 41 & 00\ 1A\ 0D\ 39 & 73\ 65\ 74\ 79 & 62\ 20\ 32\ 33 \\ 3D\ 68\ 74\ 67 & 6E\ 65\ 6C\ 20 & 2C\ 65\ 67\ 61 & 73\ 73\ 65\ 6D \end{array}$$

Аналогично находится и $A(A(V_2))$. В результате получаем

$$V_2 = A(A(V_1)) = \begin{array}{cccc} 11\ 0D\ 13\ 06 & 1D\ 16\ 09\ 4D & 0C\ 16\ 0E\ 41 & 00\ 1A\ 0D\ 39 \\ 73\ 65\ 74\ 79 & 62\ 20\ 32\ 33 & 3D\ 68\ 74\ 67 & 6E\ 65\ 6C\ 20 \end{array}$$

Теперь, для получения K_2 нужно перемешать $A(A(V_1))$ в соответствии с Таблицей 1. Получаем

$$K_2 = \begin{array}{cccc} 11\ 0C\ 73\ 3D & 0D\ 16\ 65\ 68 & 13\ 0E\ 74\ 74 & 06\ 41\ 79\ 67 \\ 1D\ 00\ 62\ 6E & 16\ 1A\ 20\ 65 & 09\ 0D\ 32\ 6C & 4D\ 39\ 33\ 20 \end{array}$$

Вычисляем U_3 по формуле $U_3 = A(U_2) \oplus C_3$. Где

$$C_3 = \begin{array}{cccc} \text{ff}\ 00\ \text{ff}\ \text{ff} & 00\ 00\ 00\ \text{ff} & \text{ff}\ 00\ 00\ \text{ff} & 00\ \text{ff}\ \text{ff}\ 00 \\ 00\ \text{ff}\ 00\ \text{ff} & 00\ \text{ff}\ 00\ \text{ff} & \text{ff}\ 00\ \text{ff}\ 00 & \text{ff}\ 00\ \text{ff}\ 00 \end{array}$$

Отсюда

$$U_3 = \begin{array}{cccc} \text{ff}\ 00\ \text{ff}\ \text{ff} & 00\ 00\ 00\ \text{ff} & \text{ff}\ 00\ 00\ \text{ff} & 00\ \text{ff}\ \text{ff}\ 00 \\ 00\ \text{ff}\ 00\ \text{ff} & 00\ \text{ff}\ 00\ \text{ff} & \text{ff}\ 00\ \text{ff}\ 00 & \text{ff}\ 00\ \text{ff}\ 00 \end{array}$$

Вычисляем V_3 по формуле $V_3 = A(A(V_2))$. Получаем

$$A(V_2) = \begin{array}{cccc} 4e\ 0d\ 00\ 1e & 0c\ 45\ 5e\ 13 & 11\ 0d\ 13\ 06 & 1d\ 16\ 09\ 4d \\ 0c\ 16\ 0e\ 41 & 00\ 1a\ 0d\ 39 & 73\ 65\ 74\ 79 & 62\ 20\ 32\ 33 \end{array}$$

$$V_3 = A(A(V_2)) = \begin{matrix} \text{7f 73 7a 38} & \text{62 3a 3f 0a} & \text{4e 0d 00 1e} & \text{0c 45 5e 13} \\ \text{11 0d 13 06} & \text{1d 16 09 4d} & \text{0c 16 0e 41} & \text{00 1a 0d 39} \end{matrix}$$

Вычисляем сумму $U_3 \oplus V_3$.

$$U_3 \oplus V_3 = \begin{matrix} \text{80 73 85 c7} & \text{62 3a 3f f5} & \text{b1 0d 00 e1} & \text{0c ba a1 13} \\ \text{11 f2 13 f9} & \text{1d e9 09 b2} & \text{f3 16 f1 41} & \text{ff 1a f2 39} \end{matrix}$$

Выполняем перемешивание

$$P(U_3 \oplus V_3) = \begin{matrix} \text{80 b1 11 f3} & \text{73 0d f2 16} & \text{85 00 13 f1} & \text{c7 e1 f9 41} \\ \text{62 0c 1d ff} & \text{3a ba e9 1a} & \text{3f a1 09 f2} & \text{f5 13 b2 39} \end{matrix}$$

Таким образом мы получили K_3. Теперь будем вычислять K_4. Вычисляем $U_4 = A(U_3) \oplus C_4$.

$$A(U_3) = \begin{matrix} \text{ff ff ff ff} & \text{ff ff ff ff} & \text{ff 00 ff ff} & \text{00 00 00 ff} \\ \text{ff 00 00 ff} & \text{00 ff ff 00} & \text{00 ff 00 ff} & \text{00 ff 00 ff} \end{matrix}$$

В этом случае

$$C_4 = \begin{matrix} \text{00 00 00 00} & \text{00 00 00 00} & \text{00 00 00 00} & \text{00 00 00 00} \\ \text{00 00 00 00} & \text{00 00 00 00} & \text{00 00 00 00} & \text{00 00 00 00} \end{matrix}$$

Получаем U_4:

$$U_4 = \begin{matrix} \text{ff ff ff ff} & \text{ff ff ff ff} & \text{ff 00 ff ff} & \text{00 00 00 ff} \\ \text{ff 00 00 ff} & \text{00 ff ff 00} & \text{00 ff 00 ff} & \text{00 ff 00 ff} \end{matrix}$$

Вычисляем $V_4 = A(A(V_3))$.

$$A(V_3) = \begin{matrix} \text{ff ff ff ff} & \text{ff ff ff ff} & \text{ff 00 ff ff} & \text{00 00 00 ff} \\ \text{ff 00 00 ff} & \text{00 ff ff 00} & \text{00 ff 00 ff} & \text{00 ff 00 ff} \end{matrix}$$

$$V_4 = A(A(V_3)) = \begin{matrix} \text{5F 00 13 18} & \text{11 53 57 5E} & \text{1D 1B 1D 47} & \text{1D 0C 04 74} \\ \text{7F 73 7A 38} & \text{62 3A 3F 0A} & \text{4E 0D 00 1E} & \text{0C 45 5E 13} \end{matrix}$$

$$U_4 \oplus V_4 = \begin{matrix} \text{A0 FF EC E7} & \text{EE AC A8 A1} & \text{E2 1B E2 B8} & \text{1D 0C 04 8B} \\ \text{80 73 7A C7} & \text{62 C5 C0 0A} & \text{4E F2 00 E1} & \text{0C BA 5E EC} \end{matrix}$$

$$K_4 = P(U_4 \oplus V_4) = \begin{matrix} \text{A0 E2 80 4E} & \text{FF 1B 73 F2} & \text{EC E2 7A 00} & \text{E7 B8 C7 E1} \\ \text{EE 1D 62 0C} & \text{AC 0C C5 BA} & \text{A8 04 C0 5E} & \text{A1 8B 0A EC} \end{matrix}$$