Московский физико-технический институт
(государственный университет)

Курс семинаров по предмету "Защита информации"
Эссе

Алгоритм Rijndael

Глаз Роман Сергеевич
Группа Б01-008а

Долгопрудный
2023

Содержание

1. Введение

Rijndael на данный момент является стандартом шифрования привительства США по результатам проведённого конкурса *Advanced Encryption Standard*, огранизованного Национальным институтом стандартов и технологий США.

Потребности принятия нового стандарта возникли из-за того, что предыдущий стандарт – *Data Encryption Standard* – имел ключ длиной всего в 56 бит, что позволяло взломать шифр простым перебором ключей.

Алгоритм Rijndael стал настолько популярным, что даже производители процессоров Intel и AMD ввели аппаратную поддержку инструкций, ускоряющих работу Rijndael.

2. Принцип работы

2.1. Краткое описание

Пусть имеется набор входных данных I и ключ K, а B – количество 32-битных слов, из которых состоят ключ и входные данные, то есть $I = (i_1, \ldots, i_B, \ldots, i_{4B})$ и $K = (k_1, \ldots, k_V, \ldots, k_{4V})$. Возможные значения B: 4, 5, 6, 7 и 8. Возможные значения V: 4, 5, 6, 7 и 8.

Rijndael сводится к следующей формальной процедуре: получить согласно некоторым правилам шифро-текст $C = (c_1, \ldots, c_B, \ldots, c_{4B})$.

Введём понятие S (state) – текущее состояние алгоритма, которое в начале соответствует входным данным I, в процессе применения алгоритма соответствует некоторому промежуточному представлению, а после применения алгоритма – шифро-тексту C. S является матрицей размером 4 x B.

Алгоритм состоит из следующих процедур:

1. Исходные данные помещаются в текущее состояние S по следующему правилу:

$$S = \begin{Vmatrix} s_{11} & s_{12} & \ldots & s_{1B} \\ \ldots & & & \\ s_{41} & s_{42} & \ldots & s_{4B} \end{Vmatrix} = \begin{Vmatrix} i_1 & i_2 & \ldots & i_B \\ \ldots & & & \\ i_{3B+1} & i_{3B+2} & \ldots & i_{4B} \end{Vmatrix} \tag{1}$$

2. К состоянию S применяется процедура трансформации – раунд (round) $N_r - 1$ раз, где N_r может принимать значения от 10 до 14 включительно в зависимости от длины ключа K (10 раз соответсвует минимальной длине ключа 128 бит и т.д.).

3. К состоянию S применяется последний раунд N_r – он немного отличается от предыдущих (подробнее об этом позже).

4. Состояние S благополучно копируется в шифро-текст C:

$$C : \begin{Vmatrix} c_1 & c_2 & \ldots & c_B \\ \ldots & & & \\ c_{3B+1} & c_{3B+2} & \ldots & c_{4B} \end{Vmatrix} = \begin{Vmatrix} s_{11} & s_{12} & \ldots & s_{1B} \\ \ldots & & & \\ s_{41} & s_{42} & \ldots & s_{4B} \end{Vmatrix} \tag{2}$$

2.2. Описание процедуры round

In progress.

3. Список используемой литературы

- TBD
- TBD