Шифрование AES

История

Был объявлен конкурс на смену DES. Всего – 15 алгоритмов.

Обязательные требования:

- размер ключей: 128, 192, 256;
- блок данных: 128.

Оценочные требования:

- криптостойкость;
- простая структура;
- нет эквивалентных ключей (различные ключи, которые дают идентичный результат шифрования);
- высокая скорость шифрования (на различных машинах);
- параллельные вычисления;
- минимальная память.

Победитель: Rijndael (разработан в Бельгийском университете) – Advanced Encryption Standard.

Advanced Encryption Standard (AES)

Слово == 32 бита (4 байта).

Входной блок данных – 4 слов. Размер ключей – 4, 6 или 8 слов.

Также имеет циклическую структуру – раунды (10, 12 или 14).

Поле Галуа

Поле Галуа GF(8) – операция сложения и умножения заменены на XOR и умножение многочленов

Пример:

$5 \cdot 7 = 101 \cdot 111$

$(x^2 + 1)(x^2 + x + 1) = x^4 + x^2 + x^3 + x + x^2 + 1 = 11011$ – *слишком большое*

Приводящий многочлен: $x^4 + 1$

Ответ: $5 \cdot 7 = 1010_2 = 10_{10}$

Расширение ключа

i - 4	i - 3	i - 2	i - 1	i			

Если 128, то заполняем первые четыре слова, потом по алгоритму:

- if i mod N_k == 0:
    - W(i - 1)
    - ShiftRow
    - SubBytes
    - XOR RCON
    - XOR W(i - N_k)
- else if N_k == 8 && i mod N_k == 4:
    - W(i - 1)
    - SubBytes
    - XOR W(i - N_k)
- else:
    - W(i - 1)
    - XOR W(i - N_k)

> Раундовый ключ всегда равен размеру блока данных

Лабораторная работа 4

Реализовать алгоритм AES.

Лекция 4 Лекция 6