# Шифрование AES

**Обязательные**

Размер ключей: 128, 192, 256 (4-6-8)

Блок данных: 128 (4 слова)

**Оценочные**

Криптостойкость

Простая структура

Нет эквивалентных ключей

Скорость

Параллельные вычисления

Минимальная память

Rijndael

Advanced Encryption Standard

Слово = 32 бита (4 байта)

Раунды 10-12-14

|  |  |  |  |
| --- | --- | --- | --- |
| А1 |  |  |  |
| А2 |  |  |  |
| А3 |  |  |  |
| А4 |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| B1 | B2 | B3 | B4 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Поле Галуа GF(8)

Сложение – xor

Умножение

5\*7=101\*111

(X^2+1)(x^2+x+1)=x^4+x^2+x^3+x+x^2+1=

11011

X^4+1

1010=10

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| i-4 |  |  | i-1 |  | i |  |  |  |  |

**? i mod Nk =0**

W(i-1)

ShiftRow

SubBytes

Xor RCON

Xor W(i-Nk)

**Nk=8 && i mod Nk=4**

W(i-1)

SubBytes

Xor W(i-Nk)

**Остальные**

W(i-1)

Xor W(i-Nk)