Symmetric Encryption

February 13, 2023

AES - Advanced Encryption Standard

- US governmental encryption standard
- Keys: choice of 128-bit, 192-bit, and 256-bit keys
- Blocks: 128 bits
- Open (world) competition announced January 97
- Standard: FIPS 197, November 2001

AES=Rijndael

- Designed by Joan Daemen and Vincent Rijmen
- Simple design, only byte operations
- S-box, substitutes one byte by another byte
- Iterated cipher

Key size	128	192	256
Number of rounds	10	12	14

AES round tranformation

Arrange the 16 input bytes in a 4×4 matrix

Subfunctions

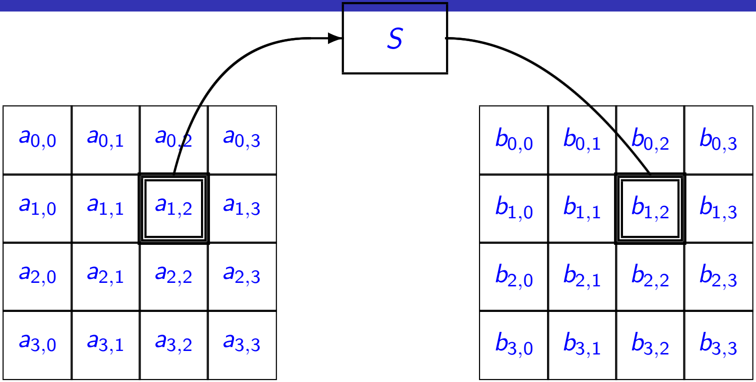
1. AddRoundKey
2. SubBytes (byte substitution via S-box)
3. ShiftRows
4. MixColumns

AddRoundKey (bit-wise XOR)

$$\begin{array}{|c|c|c|c|}\hline a_{0,0} & a_{0,1} & a_{0,2} & a_{0,3} \\ \hline a_{1,0} & a_{1,1} & a_{1,2} & a_{1,3} \\ \hline a_{2,0} & a_{2,1} & a_{2,2} & a_{2,3} \\ \hline a_{3,0} & a_{3,1} & a_{3,2} & a_{3,3} \\ \hline \end{array} \oplus \begin{array}{|c|c|c|c|}\hline k_{0,0} & k_{0,1} & k_{0,2} & k_{0,3} \\ \hline k_{1,0} & k_{1,1} & k_{1,2} & k_{1,3} \\ \hline k_{2,0} & k_{2,1} & k_{2,2} & k_{2,3} \\ \hline k_{3,0} & k_{3,1} & k_{3,2} & k_{3,3} \\ \hline \end{array} = \begin{array}{|c|c|c|c|}\hline b_{0,0} & b_{0,1} & b_{0,2} & b_{0,3} \\ \hline b_{1,0} & b_{1,1} & b_{1,2} & b_{1,3} \\ \hline b_{2,0} & b_{2,1} & b_{2,2} & b_{2,3} \\ \hline b_{3,0} & b_{3,1} & b_{3,2} & b_{3,3} \\ \hline \end{array}$$

$$b_{i,j} = a_{i,j} \oplus k_{i,j}$$

SubBytes



S

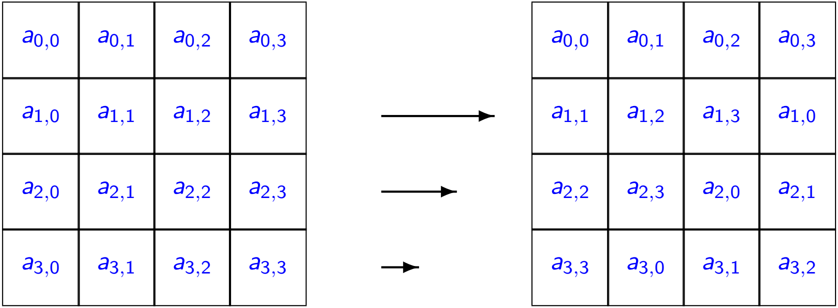
$a_{0,0}$	$a_{0,1}$	$a_{0,2}$	$a_{0,3}$
$a_{1,0}$	$a_{1,1}$	$a_{1,2}$	$a_{1,3}$
$a_{2,0}$	$a_{2,1}$	$a_{2,2}$	$a_{2,3}$
$a_{3,0}$	$a_{3,1}$	$a_{3,2}$	$a_{3,3}$

$b_{0,0}$	$b_{0,1}$	$b_{0,2}$	$b_{0,3}$
$b_{1,0}$	$b_{1,1}$	$b_{1,2}$	$b_{1,3}$
$b_{2,0}$	$b_{2,1}$	$b_{2,2}$	$b_{2,3}$
$b_{3,0}$	$b_{3,1}$	$b_{3,2}$	$b_{3,3}$

$$b_{i,j} = S(a_{i,j})$$

$S : \{0,1\}^8 \rightarrow \{0,1\}^8$ is the invertible S-box
S is a very simple non-linear function (field inversion)

ShiftRows

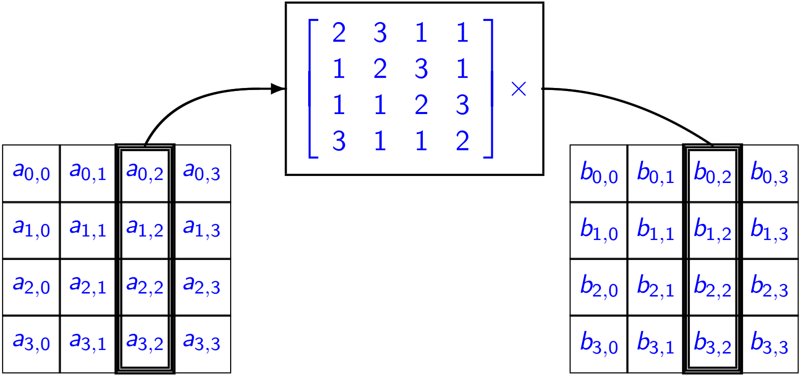


$a_{0,0}$	$a_{0,1}$	$a_{0,2}$	$a_{0,3}$
$a_{1,0}$	$a_{1,1}$	$a_{1,2}$	$a_{1,3}$
$a_{2,0}$	$a_{2,1}$	$a_{2,2}$	$a_{2,3}$
$a_{3,0}$	$a_{3,1}$	$a_{3,2}$	$a_{3,3}$

$a_{0,0}$	$a_{0,1}$	$a_{0,2}$	$a_{0,3}$
$a_{1,1}$	$a_{1,2}$	$a_{1,3}$	$a_{1,0}$
$a_{2,2}$	$a_{2,3}$	$a_{2,0}$	$a_{2,1}$
$a_{3,3}$	$a_{3,0}$	$a_{3,1}$	$a_{3,2}$

Rows shifted over different offsets: 0,1,2, and 3

MixColumns



$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \times$$

$a_{0,0}$	$a_{0,1}$	$a_{0,2}$	$a_{0,3}$
$a_{1,0}$	$a_{1,1}$	$a_{1,2}$	$a_{1,3}$
$a_{2,0}$	$a_{2,1}$	$a_{2,2}$	$a_{2,3}$
$a_{3,0}$	$a_{3,1}$	$a_{3,2}$	$a_{3,3}$

$b_{0,0}$	$b_{0,1}$	$b_{0,2}$	$b_{0,3}$
$b_{1,0}$	$b_{1,1}$	$b_{1,2}$	$b_{1,3}$
$b_{2,0}$	$b_{2,1}$	$b_{2,2}$	$b_{2,3}$
$b_{3,0}$	$b_{3,1}$	$b_{3,2}$	$b_{3,3}$

Bytes in columns are combined linearly

$$b_{0,2} = \{2\} \times a_{0,2} \ + \ \{3\} \times a_{1,2} \ + \ \{1\} \times a_{2,2} \ + \ \{1\} \times a_{3,2}$$

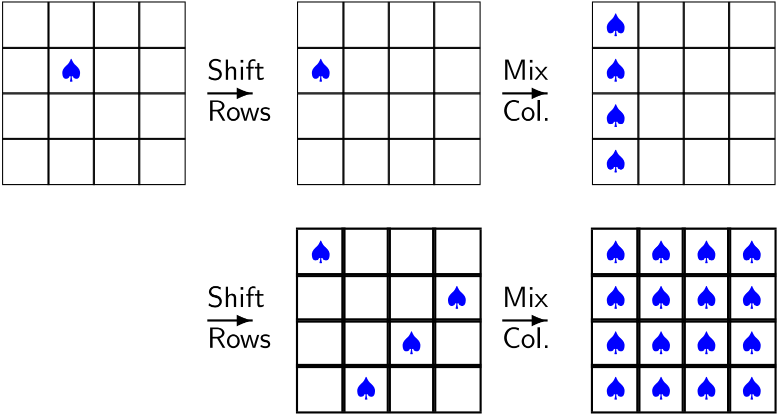
Multiplication is a special field-multiplication

AES - 10-round version

Arrange the 16 input bytes in a 4×4 matrix

- AddRoundKey
- Do nine times
    - SubBytes (byte substitution via S-box)
    - ShiftRows
    - MixColumns
    - AddRoundKey
- SubBytes
- ShiftRows
- AddRoundKey

Byte mixing in AES



Shift Rows

Mix Col.

Shift Rows

Mix Col.

Modes of operation for block ciphers

Block cipher with n-bit blocks, e.g. DES: $n = 64$, AES: $n = 128$

Message m split into blocks of n bits, i.e.,

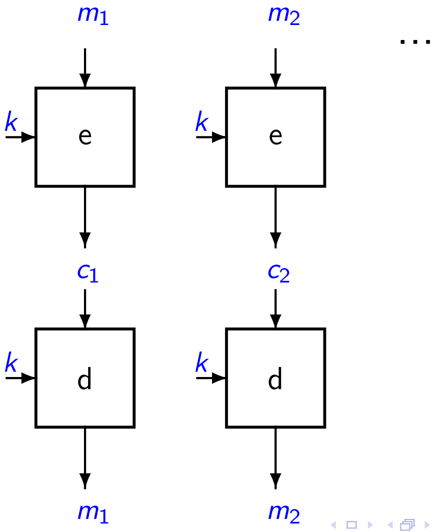
$$m = m_1, m_2, \ldots, m_t,$$

where $|m_i| = n$

Many modes of operation: ECB (dangerous, don't use), CBC, CFB, OFB, CTR, GCM...

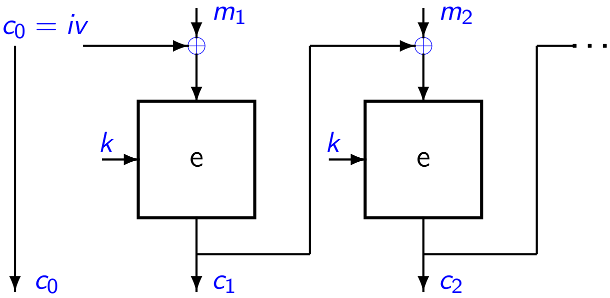
ECB mode (dangerous, don't use)

Encryption and decryption



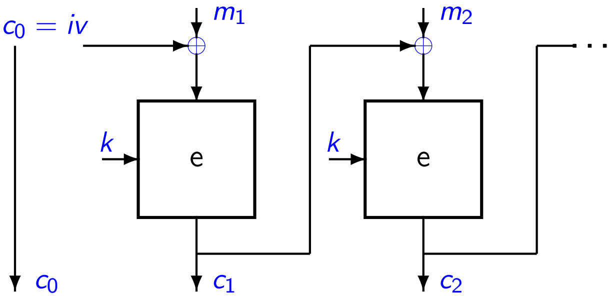
CBC mode

Encryption



CBC mode

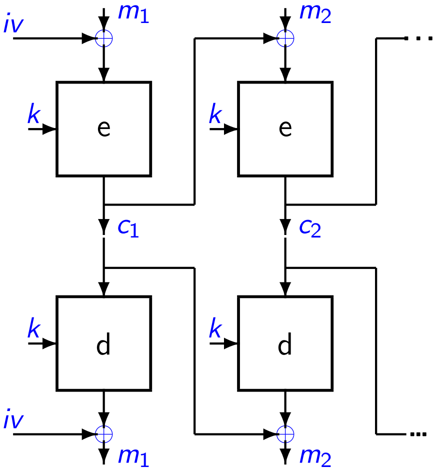
Encryption



How does decryption work?

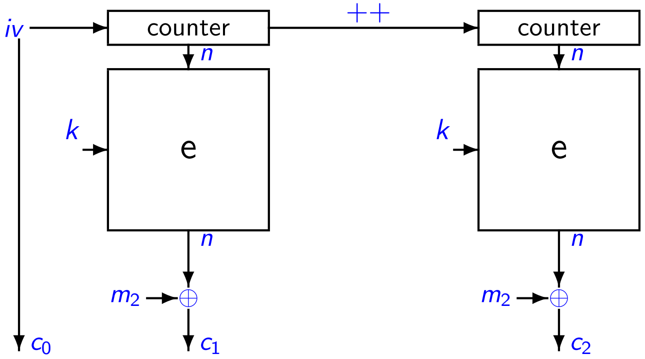
CBC mode

Encryption and decryption



CTR mode

n and m are sizes in bits


iv
counter
$++$
counter
n
n
k
e
k
e
n
n
m_2
m_2
c_0
c_1
c_2