# Advanced Encryption Standard

Murat Kantarcioglu

## History of AES

- Due to limitations of DES (small key and block sizes), NIST started a open process to select a new block cipher.
- 15 proposals submitted to NIST around 1998.
- Rijndael from Belgium chosen as the AES in 2001 after an open process.
- Rijndael is chosen because of its security, performance, efficiency, implementability, and flexibility.

# Overview of AES

- AES is not Feistel Network.
- AES is a type of SPN
- AES has 128 bits block size
- AES has three allowable key sizes |K|={128,192,256}
- AES has variable number of rounds
  - If |K|=128 then Nr=10
  - If |K|=192 then Nr=12
  - If |K|=256 then Nr=14

# AES: High Level Description

$AES(K, M)$ $//|K| \in \{128, 192, 256\}$
{
  state $\leftarrow M$
  $(K_0, \ldots, K_{Nr}) \leftarrow Keys(K)$
  state $\leftarrow K_0 \oplus state$
  for $r = 1$ to $Nr$
   {
    subbytes(state,S-box)
    shiftrows(state)
    if $r \leq Nr - 1$ then mixcloumn(state,S-box)
    state $\leftarrow K_r \oplus state$
   }
  return $c \leftarrow$ state
}

# State in AES

- All operations in AES are byte oriented.
- A plaintext consists of 16 bytes $(m_0, \ldots, m_{15})$
- Initially State is defined as follows:

| | | | |
|---|---|---|---|
| $S_{0,0}$ | $S_{0,1}$ | $S_{0,2}$ | $S_{0,3}$ |
| $S_{1,0}$ | $S_{1,1}$ | $S_{1,2}$ | $S_{1,3}$ |
| $S_{2,0}$ | $S_{2,1}$ | $S_{2,2}$ | $S_{2,3}$ |
| $S_{3,0}$ | $S_{3,1}$ | $S_{3,2}$ | $S_{3,3}$ |



| | | | |
|---|---|---|---|
| $m_0$ | $m_4$ | $m_8$ | $m_{12}$ |
| $m_1$ | $m_5$ | $m_9$ | $m_{13}$ |
| $m_2$ | $m_6$ | $m_{10}$ | $m_{14}$ |
| $m_3$ | $m_7$ | $m_{11}$ | $m_{15}$ |

- Round Key addition xors the round key with 16bytes state.

# Subbytes()

- AES byte substitutions are done using non-linear S-boxes.
- S-box are represented as 16x16 array where rows and columns are represented as hexadecimal arrays.
- Write a byte as two hexadecimal numbers and r,c and return $s_{r,c}$

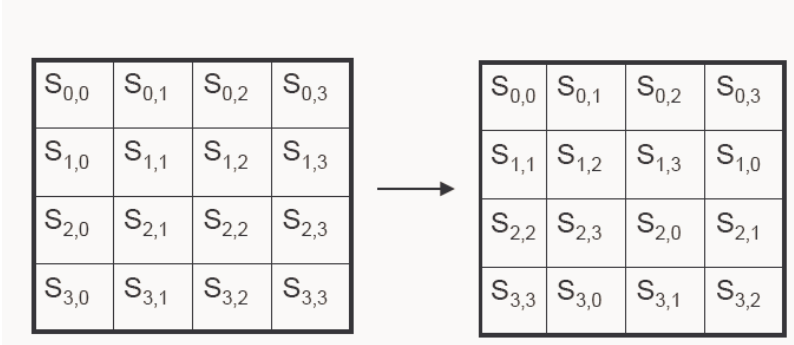
## Subbytes()

- Unlike DES, the design choices for AES S-box is clear.
- It is designed to prevent linear and differential cryptanalysis.
- It can be represented as a set of algebraic operations in the finite field $\mathcal{F}_{2^8}$

## Subbytes()

subbytes(a)
{
  $z \leftarrow$ binarytofield(a)
  if $z \neq 0$ then $z \leftarrow$ fieldinv(z)
  $a \leftarrow$ fieldtobinary(z)
  $c \leftarrow 01100011$
  for $i = 0$ to 7
   {
    $b_i \leftarrow (a_i + a_{i+4} + a_{i+5} + a_{i+6} + a_{i+7} + c_i) \bmod 2$
   }
  return $b$
}

# ShiftRows()




# MixColumns

- Each column is represented as a 4 byte vector
- Each column of State is replaced by a new column which is formed by multiplying that column by a certain matrix of elements of the field $\mathcal{F}_{2^8}$
- We can also see this operation as polynomial multiplication where each column is represented with polynomial a(x)

$$\begin{aligned} a(x) &= c(x).a(x) \bmod x^4 + 1 \\ &= (\{03\}x^3 + \{01\}x^2 + \{01\}x + \{02\}) \\ &\quad .(a_3x^3 + a_2x^2 + a_1x_1 + a_0) \bmod x^4 + 1 \end{aligned}$$

# KeyExpansion

```
KeyExpansion(byte key[4*Nk], word w[Nb*(Nr+1)], Nk)
begin
   word  temp

   i = 0

   while (i < Nk)
      w[i] = word(key[4*i], key[4*i+1], key[4*i+2], key[4*i+3])
      i = i+1
   end while

   i = Nk

   while (i < Nb * (Nr+1)]
      temp = w[i-1]
      if (i mod Nk = 0)
         temp = SubWord(RotWord(temp)) xor Rcon[i/Nk]
      else if (Nk > 6 and i mod Nk = 4)
         temp = SubWord(temp)
      end if
      w[i] = w[i-Nk] xor temp
      i = i + 1
   end while
end
```

# KeyExpansion

$$RotWord(B_0, B_1, B_2, B_3) = (B_1, B_2, B_3, B_0)$$

$$SubWord(B_0, B_1, B_2, B_3) = (subbytes(B_0), subbytes(B_1), subbytes(B_2), subbytes(B_3))$$

## Decryption

- Suggested Approach: Perform all operations in reverse order and use the key schedule in reverse order.
- Note that each step is invertible.

## Security of AES

- Resistant to all known attacks
  - i.e., linear and differential cryptanalysis
- Designed to make sure that different tables and linear approximations are close to uniform distribution (e.g., inverse operation)
- No known attack on the 10 round version better than exhaustive key search
- One criticism : AES could be written as a simple algebraic set of equations..


# Summary

- AES is chosen after an open contest.
- The design choices are clear.
- No known attack against it at the moment.
- AES is supported by almost all vendors.