CIS 3362 9/29/25

Please look at DES code for any further clarifcation on the algorithm or key schedule.

mid 1990s computers getting faster
1998 DES Challenge
Distributed - you download program, your computer was idle, it would try some keys.
~ 3 months key was broken.

NIST offered a new contest for a new symmetric block cipher system to be the US Govt Standard.
15 applicants → 5 finalist → winner

Criteria: 1. Secure so block size had be larger
2. Fast
3. Simple

Rijndael was winner named after 3 inventors
John Daemen, Vincent Rijmen (Belgium)

3 Versions: 128-bit, 192-bit, 256-bit

Also a block cipher in rounds.

16 bytes

The algorithm has a basis in number theory but you don't have to understand the number theory to be able to trace the steps. (MixCols forces you to understand a little bit of it.)

$GF(2^8) \mod x^8 + x^4 + x^3 + x + 1$

10 rounds

In most rounds we have 4 steps

SubBytes
ShiftRows
MixCols
AddRoundKey

Algorithm

Input: P Output: C

1. $S = \text{AddRoundKey}(P, K_0)$

2. for $i = 1$ to 9
   $S = \text{SubBytes}(S)$
   $S = \text{ShiftRows}(S)$
   $S = \text{MixCols}(S)$
   $S = \text{AddRoundKey}(S, K_i)$

3. $S = \text{SubBytes}(S)$
   $S = \text{ShiftRows}(S)$
   $S = \text{AddRoundKey}(S, K_{10})$

} in round 10 skip MixCols.

4. Return S

128 bits
128 bits

State matrix

P

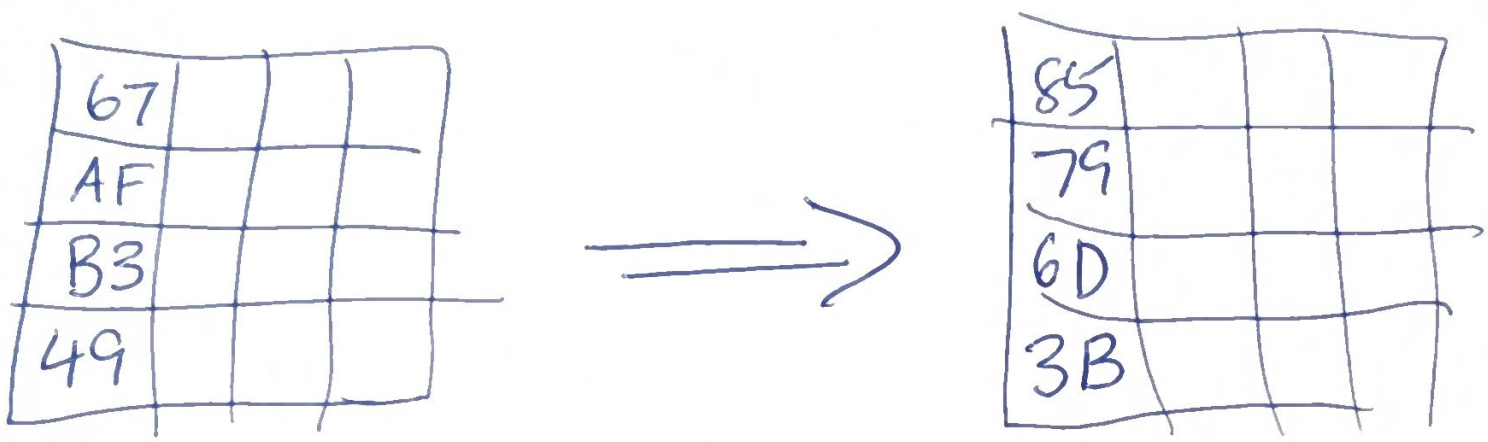
$b_{0,0}$	$b_{0,1}$	$b_{0,2}$	$b_{0,3}$
$b_{1,0}$	$b_{1,1}$	$b_{1,2}$	$b_{1,3}$
$b_{2,0}$	$b_{2,1}$	$b_{2,2}$	$b_{2,3}$
$b_{3,0}$	$b_{3,1}$	$b_{3,2}$	$b_{3,3}$

Order of bytes $b_{0,0}, b_{1,0}, b_{2,0}, b_{3,0}$
$b_{0,1}, b_{1,1}, b_{2,1}, b_{3,1}$
b

Sub Bytes

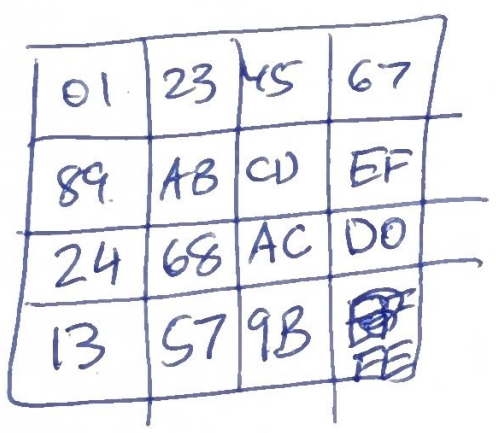
look up each byte in the byte substitution table.

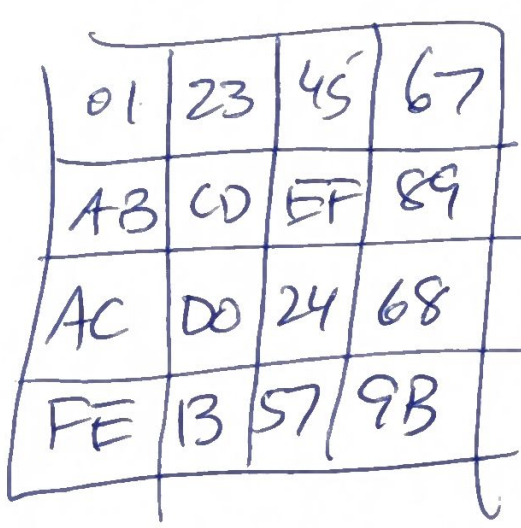
How to read AES S-box.



SubBytes(67), go to row 6, col 7 in the S-box

Shift Rows





Same

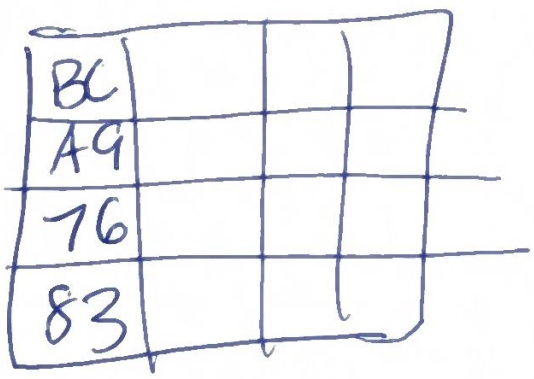
left cyclic shift 1 byte

= = shift 2 byte

= = = 3 bytes

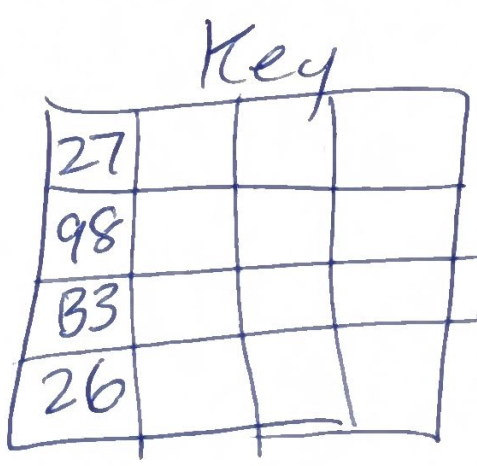
Add Round Key is JUST an XOR

State Matrix

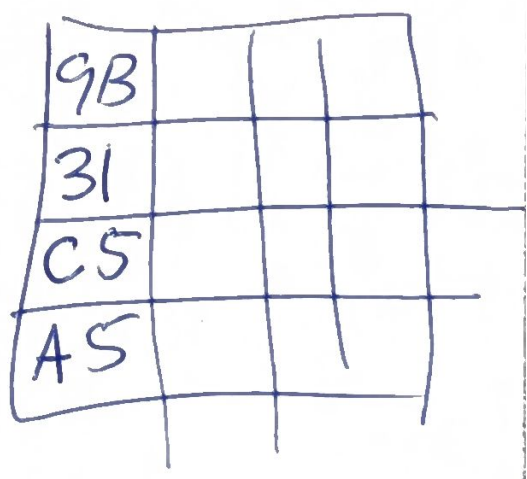


⊕

Key



=



BC⊕27 = 9B (use Hex XOR table)

Math (Some) behind AES

Normally, a byte is 8 0s or 1s.
But in AES, a byte represents a polynomial where all coefficients are 0 or 1 MOD the polynomial $x^8 + x^4 + x^3 + x + 1$. This polynomial is irreducible, the meaning that no 2 polynomials with coefficients under mod 2 both with degree 1 or greater multiply to it.

$$(x^2 + x + 1)(x^3 + 1)$$
$$= x^5 + x^4 + x^3 + x^2 + x + 1$$

$$(x^2 + 1)(x^2 + x + 1)$$
$$= x^4 + x^3 + x^2$$
$$+ x^2 + x + 1$$
$$= x^4 + x^3 + 2x^2 + x + 1$$
$$= x^4 + x^3 + x + 1 \quad \text{(each coeff is mod 2)}$$

To calculate $p(x)$ mod $q(x)$, divide $q(x)$ into $p(x)$ get a quotient function and then a remainder $r(x)$ will be leftover of degree less than the degree of $q(x)$.

$x^8 + x^4 + x^3 + x + 1$ ÷ $x + 1$ — quotient

$$x^9 + x^8 + x^3 + 1$$
$$-(x^9 + x^5 + x^4 + x^2 + x)$$
$$x^8 + x^5 + x^4 + x^3 + x^2 + x + 1$$
$$-(x^8 + x^4 + x^3 + x^2 + x)$$
$$x^5 + 1$$

remainder

$GF(2^8)$ mod $x^8 + x^4 + x^3 + x + 1$

0000 0100

$x^7\ x^6\ x^5\ x^4\ x^3\ x^2\ x^1\ x^0$

for us memorize that

$x^8 \mod x^8 + x^4 + x^3 + x + 1 = x^4 + x^3 + x + 1$ ↵

0001 1011

$x^{10} + x^9 \mod x^8 + x^4 + x^3 + x + 1$

$= x^2(x^8) + x(x^8) \mod x^8 + x^4 + x^3 + x + 1$

$\equiv (x^2 + x)(x^8) \mod x^8 + x^4 + x^3 + x + 1$

$\equiv (x^2 + x)(x^4 + x^3 + x + 1) \mod x^8 + x^4 + x^3 + x + 1$

$= x^6 + x^5 + x^3 + x^2 + x^5 + x^4 + x^2 + x = x^6 + x^4 + x^3 + x$

Mix Cols

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} 01 & 23 & 45 & 67 \\ 89 & AB & CD & EF \\ FE & DC & BA & 98 \\ 76 & 54 & 32 & 10 \end{bmatrix}$$

Do this matrix mult

row 3 col 2 = $01\times23 + 01\times AB + 02\times DC + 03\times 54$

using 1-based indexing

$01\times23 = 23$

$01\times AB = AB$

$02\times0C = AB$

$03\times54 = FC$

D7

poly x

$02\times DC$ = (overflow bit) 1 01 11000 // mult by 2

$= 100000000 + 10111000$

$= 00011011 \pmod{AES\ poly}$

$\oplus\ 10111000$

10100011

A 3

$x+1$

$03\times54 =$

$(02+01)\times54 =$

$02\times54 + 01\times54$

$0101\ 0100$

$\oplus\ 1010\ 1000$

$1111\ 1100$

F C