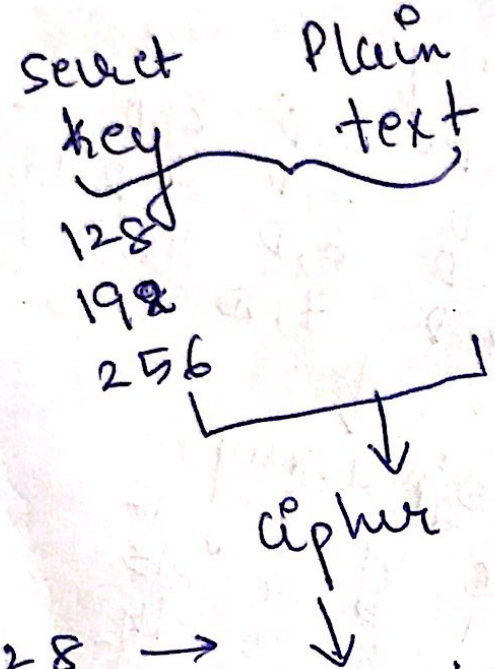
Advanced Encryption standard.

1) 10 rounds



128 → 10 rounds → cipher text

192 → 12 rounds

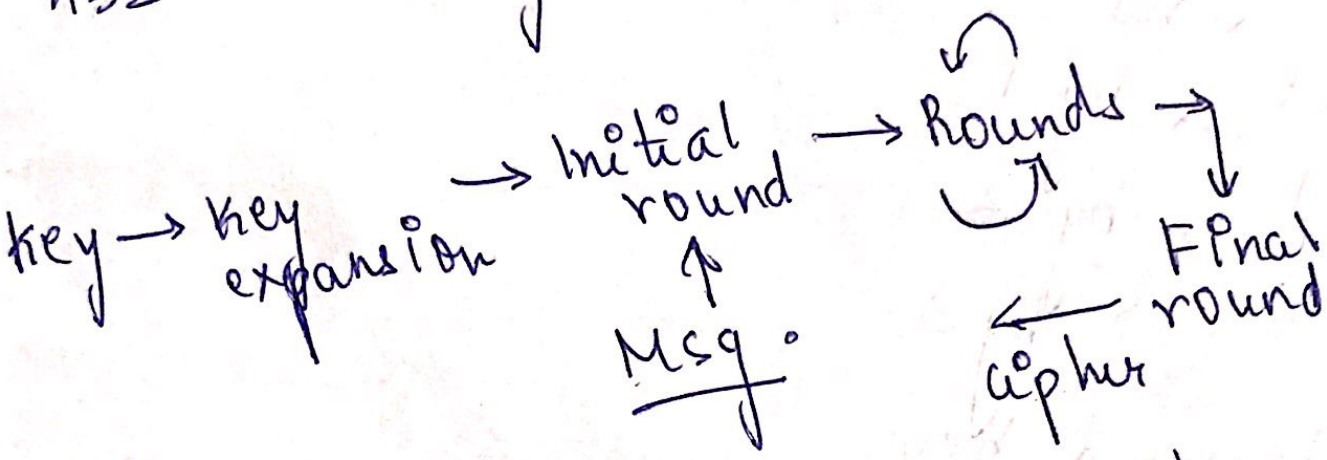
256 → 14 rounds. [Last round 10th, 12th, 14th is different.

Rounds
→ subbytes
→ shift rows
→ Mix columns
→ Add round key

common key length	block size	Rounds
128	4	10
192	6	4
256	8	4

slower by far more secure.

Msg 425, 7 byte padding to make 432
432 divisible by 16



Key Expansion
Alters original key such that it is different in each round.
Encrypts the key itself.

AES Encryption
I/P → msg and key

Sub bytes
uses a look up table (S box)
byte hex
row column } replace by value there

state example
what is reel?

w a e
h i e
a s c i
t r s

→ state.

shift rows. → Rotate left

1st → no

2nd → by 1

3rd → by 2

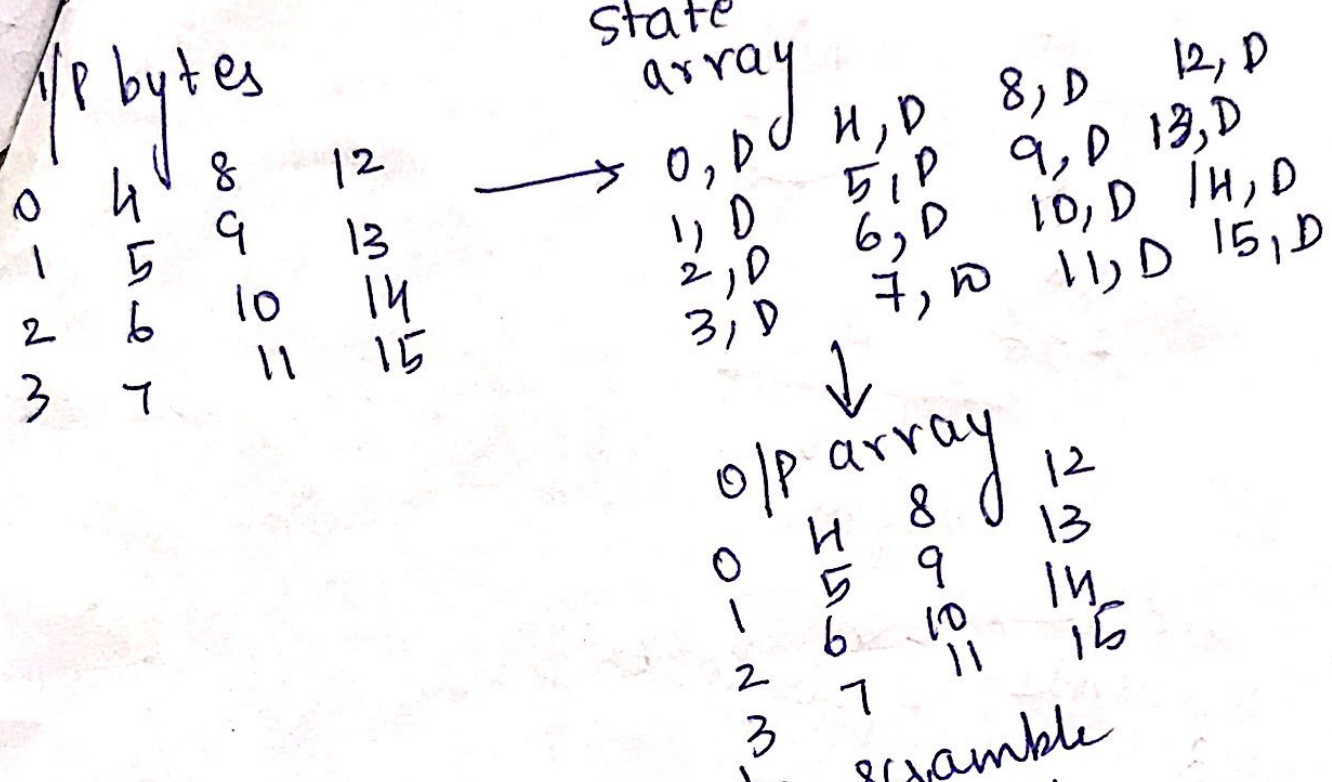
4th → by 3

Addround key

Xor with round key

In the 10th round mix column is eliminated

Algorithm happens on 2D array called as state



A same key is used to scramble the data to send it over the n/w and can be unscrambled using the same over the reciever end.

Small key length of DES could be broken using parallel computing brute force.

AES encrypts 128 bits of data

Treats 16 byte as 4 X 4 matrix.

Msg greater than 128 bits are broken to blocks and encrypted seperately

Mix columns

→ Dot product
→ Matrix Multiplication
Polynomial multiplication Mod 2

11010110 * 00 11 01 10
$(x^7 + x^6 + x^4 + x^2 + x^1) * (x^5 + x^4 + x^2 + x^1)$
row * column

simple method

[Add]

	1	2	4	5
1	2	3	5	6
2	3	4	6	7
4	5	6	8	9
6	7	8	10	11
7	8	9	11	12

Mod 2 now apply → 0 → even no
→ 1 → odd no.

If bit has even number (Even no bit) in grid replaced by 0

12 11 10
1010 10 0 0 1 0 0
9 8 7 6 5 4 3 2 1 0

not present

Doesnot fit into a byte (not 8 bit)

Reduction mod $x^8 + x^4 + x^3 + x^1 + 0$

Divide by this and take remainder to get a byte.

$x^8 + x^4 + x^3 + x^1 + 0$

100011011.

Do long division.

Subtraction mod 2 [XOR]

```
  10 10 10 10 10 100
⊗ 10 00 11 01 1
-------------------
  00 1 0 0 1 1 1 0 0 1 0 0
```

Ans larger/smaller than magic byte

If larger repeat

```
  100 111 00 100
⊕ 100 011 01 1
-------------------
  00 0 1 0 0 0 1 0 0 0
```

$\longrightarrow$ smaller

$10001101 1$

$1000 1000 \longrightarrow$ remainder.

Example

X57
0X68 ∘ 0X02 0X03 0X01 0X01
X61
X74

57 → 010.10.111. X 10

$x^6 + x^4 + x^2 + x^1 + x^0 \times x^1$

0	1
1	2
2	3
4	5
6	7

Only odd nos → 01
Mod no.

Ans

10101110 → 8 digit

no need of reduction as the no. is less than magic no.

10001101 → magic no.
10101110

68 x 3

(D 11a 1000) x (11)

$(x^6 + x^5 + x^3)(x^1 + x^0)$

	1	0
6	7	6
5	6	5
3	4	3

Mod 2 → odd → 1
Even → 0

10111000. → Ans

Magic no. 10001011 is bigger.

or you can bookup in wikipedia

→ Ans

5 7
↓ ↓
row column

61 x 1 → 61

74 x 1 → 74

Step 2 is xor

```
1 0 1 0 1 1 1 0
⊗ 1 0 1 1 1 0 0 0      odd no. of 1s → 1
  0 1 1 0 0 0 0 1      Even no. of
  0 1 1 1 0 1 0 0      1s → 00
  ---------------
  0 0 0 0 0 0 1 1
```

Ans 3

Matrix Multiplication

$$\begin{bmatrix} 1 & 5 & 9 & 13 \\ 2 & 6 & 10 & 14 \\ 3 & 7 & 11 & 15 \\ 4 & 8 & 12 & 16 \end{bmatrix} \times \begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix}$$

(Right shift)

AES Key Expansion

Expand Key into 10 new Key one for each round.

Key Expansion core → Rotate
→ S-box
→ Rcon

w[i-4] ——— w[i-1]

2b 28 ab 09
Te ac f7 cf
15 d2 15 4f
16 a6 88 3c

Columns which are multiples of 4 are filled in special.

→ Rotate the previous column by 1
→ Apply the s box.
→ xor the 1st row with the modified w[i-4] transformed row obtained above and RCON(i).

→ Each w depends on w[i-1] and w[i-4]

$rcon(i) = x^{i-1} \bmod x^8 + x^4 + x^3 + x^1 + 1$

$rcon(10) = x^9 \bmod x^8 + x^4 + x^3 + x^1 + 1$

where i is the round

1 0 0 0 0 0 0 0 0
⊕ 1 0 0 0 1 1 0 1 1 ↓
0 0 0 0 1 1 0 1 0 .

5 4 3 2 1

$x^5 + x^4 + x^2 + x$

0 x 36

Rcon matrix → [rcon(i) 0 0 0]

Example

0x57
0x6a
0x6
0x

Other ... $w_i \rightarrow w_{i-1} \oplus w_{i-4}$

No. of Key expansions = No. of rounds + 1