Securité

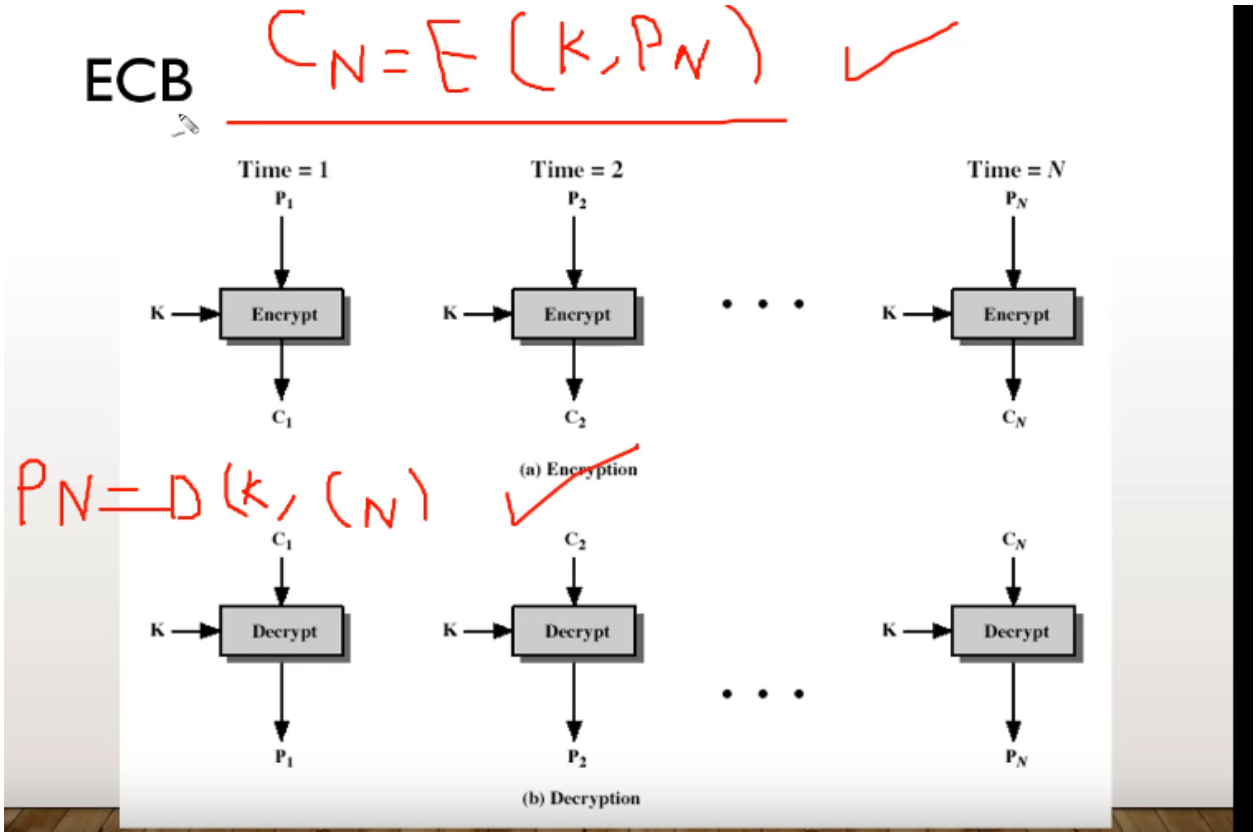
Caesar :
Encryption F(Plain, Key) = (P+K) MOD 26
Decryption F(Cipher,Key) = (C-K) MOD 26

Key= F(Plain,Cipher) = (C-P) Mod 26

PlayFair :

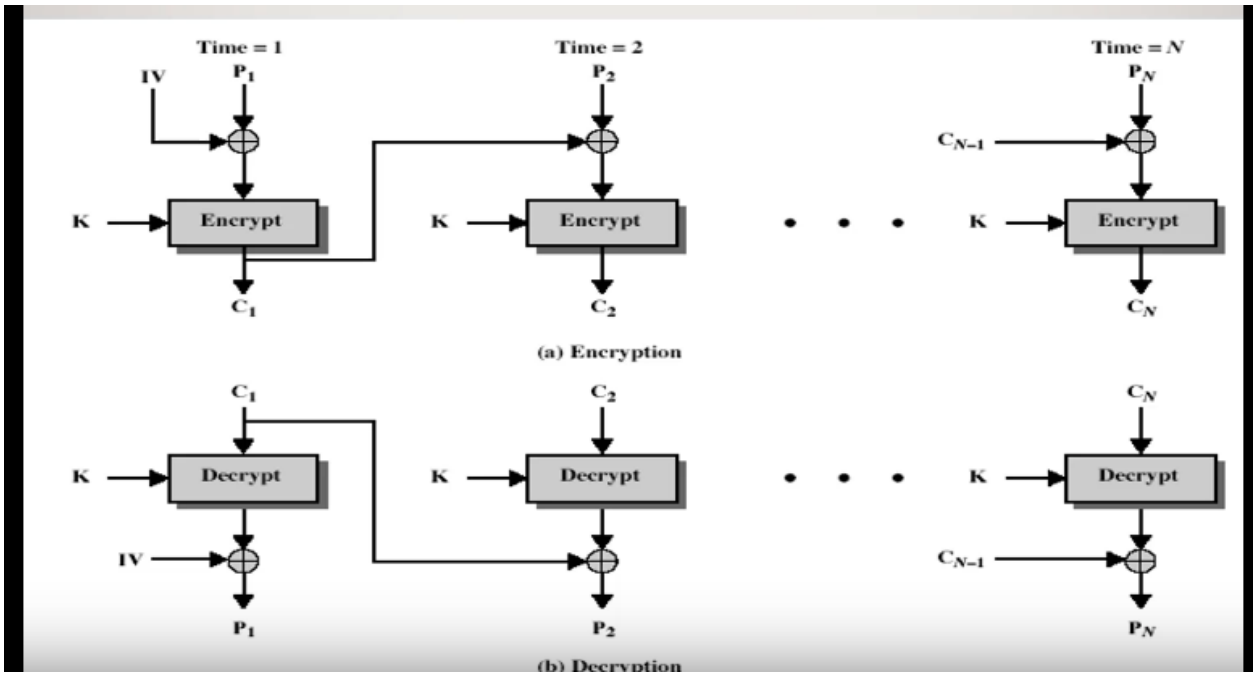
- Row of letter and column of the other
- Separator X
- Filler X
- In case same Row :
  - Encryption : Shift right
  - Decrypt : Shift left
- In case same column :
  - Encryption : Shift down
  - Decrypt : Shift up

Operation modes for DES and AES :
ECB : Electronic Codebook Book mode



- +ECB can be done simultaneously (threads)
- +Order doesn't matter in ECB
- ECB is suitable for short messages (IVs) or for exchanging keys of other modes
- -La redondance des memes blocs est propagé

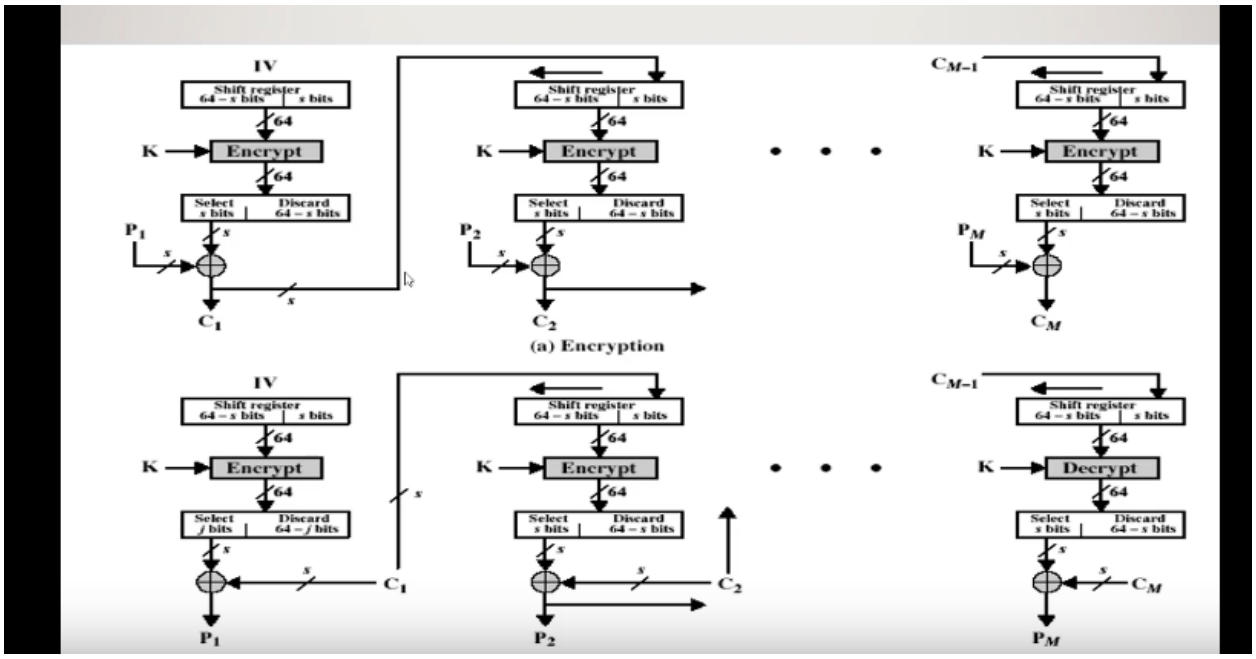
CBC : Cipher Block Chaining mode



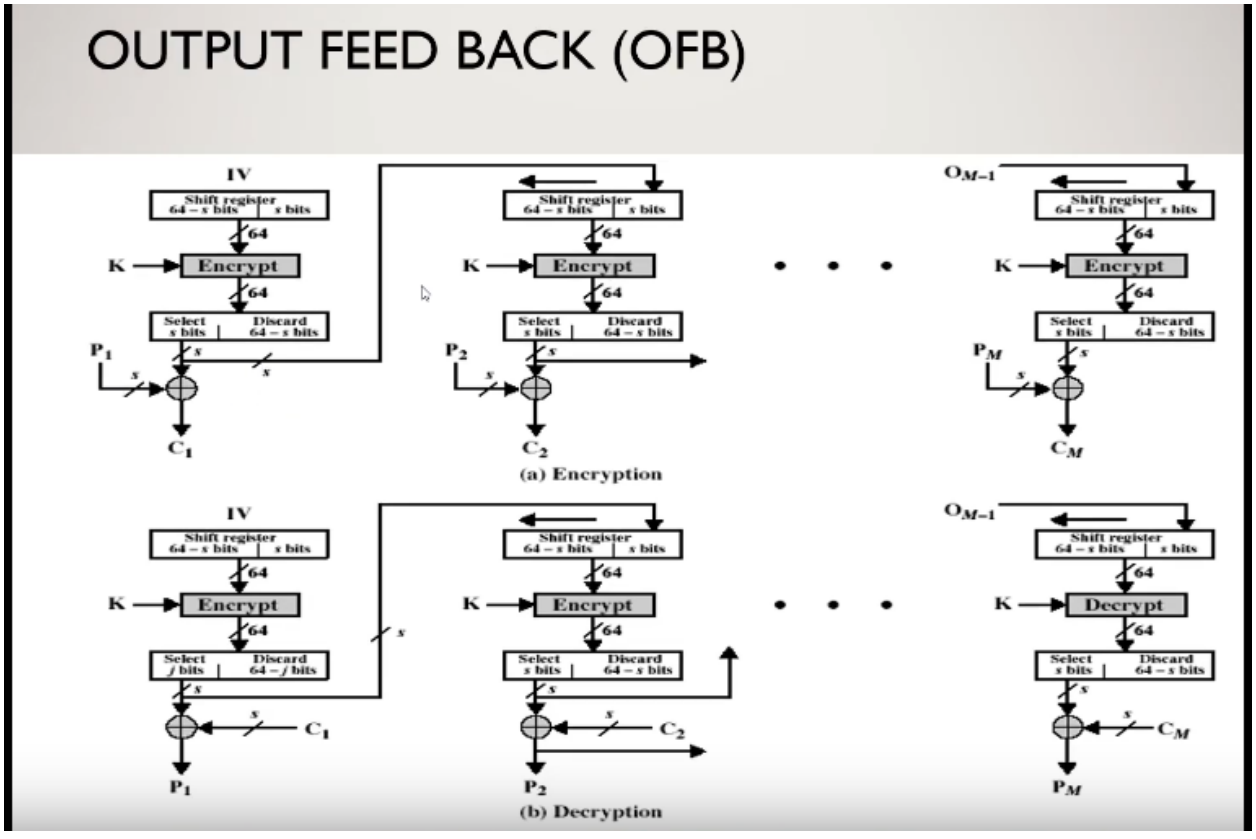
Cryptage :
C 0 = IV ; c j =E(c j-1 ⊕ m j) pour 1 ≤ j ≤ t
Décryptage :
C 0 = IV ; m j = c j-1 ⊕ D(c j) pour 1 ≤ j ≤ t

- +Plus de confusion
- +Si l'ordre change le decryptage devient impossible
- -Propagation de l'erreur
- Approprié au messages longs (Multimedias)

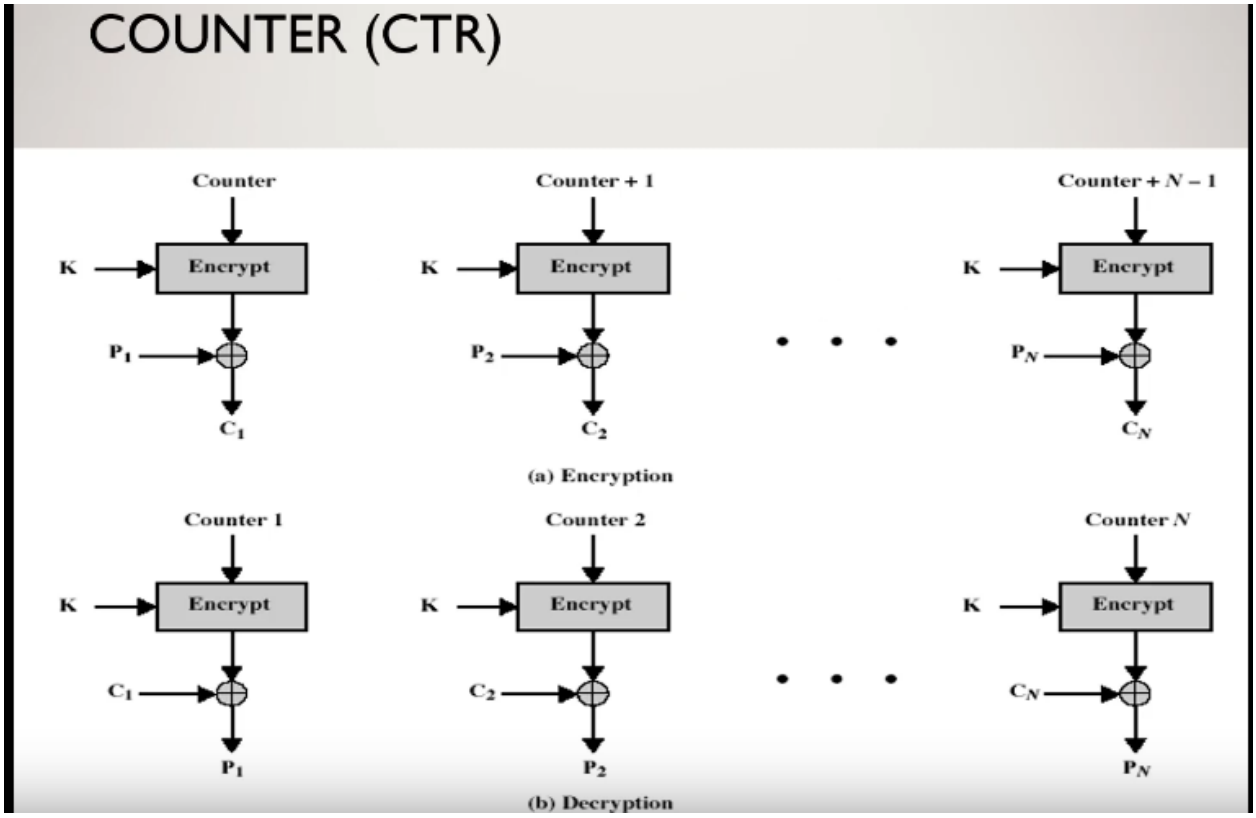
CFB Cipher Feed Back Mode



OFB Output Feed Back Mode



Counter Mode :



Parameters d'un algo de cryptage :
confusion : Rend la relation entre le ciphertext et la clé aussi complexe que possible (apparence aléatoire)
diffusion : Chaque bit du plaintext affecte tous les bits du ciphertext (avalanche)

DES :
IP MATRIX

48 bits

Initial Permutation (IP)

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

Expansion MAtrix

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

RSA:
1 - Choose 2 prime numbers p and q
2 - Compute N = p x q
3 - Compute Phi(N) = (p-1)(q-1)
4 - Choose e
1 < e < phi and must be coprime with phi (PGCD(e,phi) = 1)
Choose d
0 ≤ d ≤ n
D = (1 + k*phi)/ e and K : 1 .. e The result should be prime and no decimal
Public key (e,n)
Private Key (d,n)

Taille maximale d'un bloc de plaintext X = Entiere(Ln(n)/ln(dimension(text clair))
Taille maximale d'un bloc de cipher = X+1

Encryption
E(P) = P^e mod n
Decrypt

D(C) = C^d mod n

Diffie Helmann
Soit p =17, g= 3 des clés globales partagés entre Alice et bob.
Alice choisit a= 7, et Bob choisit b= 4.

- Alice calcule sa clé publique A = g^a mod p = 3 7 mod 17 = 11 et envoie A à Bob
- Bob calcule sa clé publique B = g^b mod p = 3 4 mod 17 = 13 et envoie B à Alice
- Alice calcule la clé secrète par K = B^a mod p = 13 7 mod 17 = 4
- Bob calcule la clé secrète K par K = A^b mod p = 11 4 mod 17 = 4