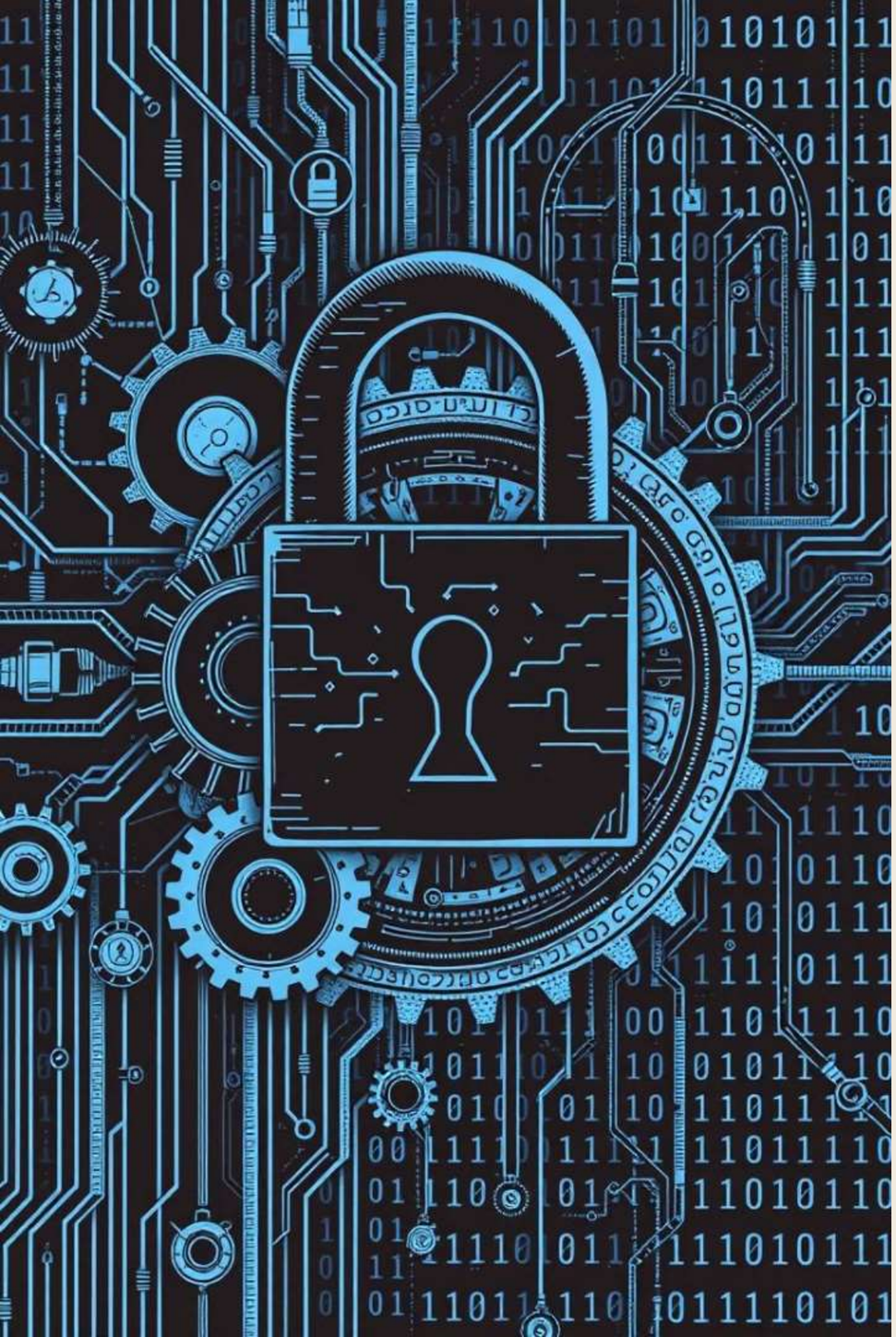
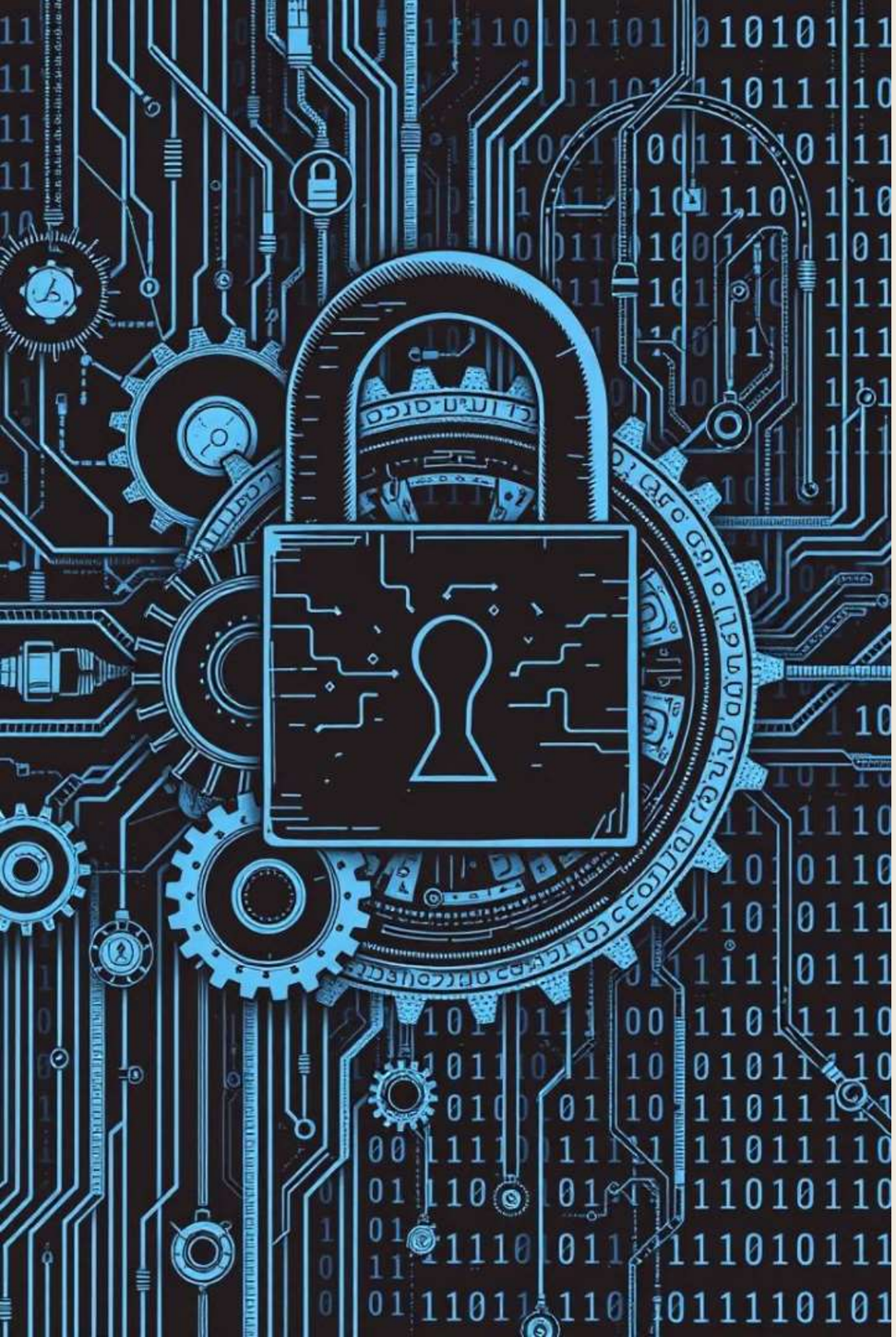


Cours
Sécurité Informatique
L3 : SI & ISIL

Bienvenue à ce cours sur la sécurité informatique.
Préparez-vous à explorer des concepts complexes et des technologies révolutionnaires qui sous-tendent la sécurité numérique moderne.

Dr F.Khalifa
Université USTOMB
2024-2025



Sécurité Informatique

Chapitre 3:
Cryptographie Moderne

Chiffrement Symétrique

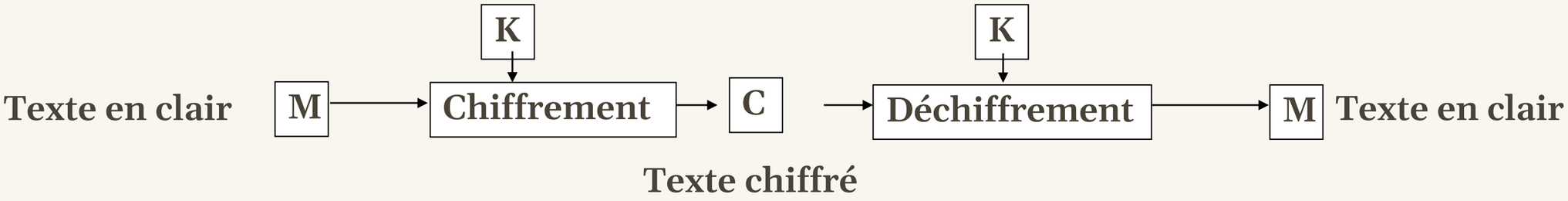
Dr F.Khalifa

Université USTOMB

2024-2025

Chapitre 3: Cryptographie moderne
Chiffrement Symétrique

Introduction



En cryptographie, la propriété de base est que : M = D(E(M)) où
– M représente le texte en clair
– C est le texte chiffré,
– K est la clé
– E(x) est la fonction de chiffrement
– D(x) est la fonction de déchiffrement.
Ainsi, avec un algorithme à clef symétrique, M = D(C) si C = E(M)

Chapitre 3: Cryptographie moderne
Chiffrement Symétrique

Introduction

Dans la cryptographie symétrique, la clé de chiffrement est la même que la clé de déchiffrement. La clé est donc un secret partagé uniquement entre l'émetteur et le destinataire. Il existe plusieurs algorithmes de chiffrement symétrique : DES, RC4, RC5, Blowfish, IDEA, AES, ….

La cryptographie symétrique utilise deux types de chiffrement manipulant des mots binaires :

- **Le chiffrement par flot : le message est traité bit par bit**
  Algorithmes :RC4, Bluetooth E0/1, GSM A5/1

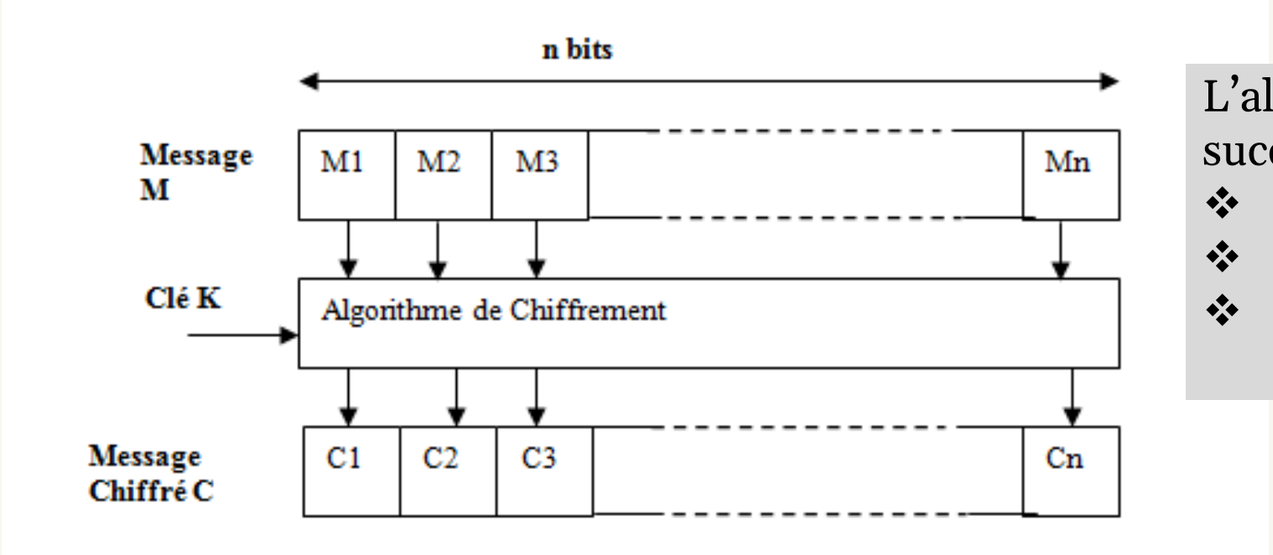
- **Le chiffrement par bloc**

Chapitre 3: Cryptographie moderne

Chiffrement Symétrique

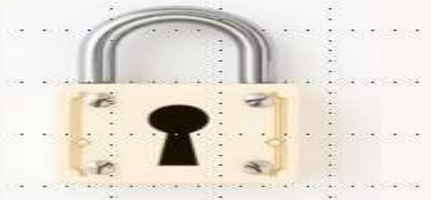
Chiffrement par bloc

Le chiffrement par bloc consiste à découper le message à chiffrer en bloc de taille fixe (exemple : 64 bits). Puis appliquer l'algorithme de chiffrement sur chaque bloc. On découpe le message M de n bits en s blocs de l = n/s bits (on ajuste initialement la taille du message en ajoutant des caractères sans signification afin que sa taille soit un multiple de l). Un algorithme de chiffrement par blocs opère sur des blocs de l bits, pour produire en général un bloc de l bits afin d'assurer la bijectivité du code.



L'algorithme de chiffrement (K) est en général une succession des opérations suivantes:

- Permutation
- Substitution
- Opération XOR (Ou Exclusif)



Chapitre 3: Cryptographie moderne

Chiffrement Symétrique

Modes opératoires

On distingue plusieurs modes opératoires utilisés dans le chiffrement par bloc.
Dont les plus courants sont :

- Le mode Electronic Code Book (ECB)
- Le mode Cipher Block Chaining (CBC)
- Le mode Cipher Feedback (CFB)
- Le mode Output Feedback (OFB)

Chapitre 3: Cryptographie moderne

Chiffrement Symétrique

Modes opératoires

Le mode Electronic Code Book (ECB)

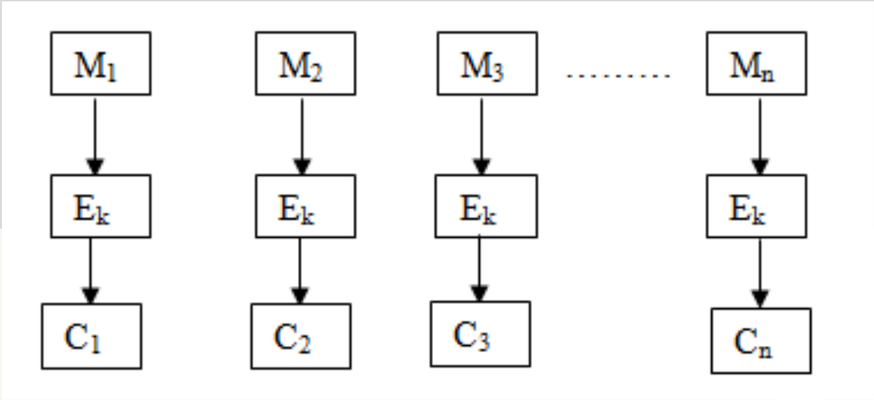
Dans ce mode, le message M est découpé en blocs mi de taille fixe.

Chaque bloc est alors chiffré séparément par une fonction, paramétrée par une clé k. Ainsi un bloc de message donné « m_i » sera toujours codé de la même manière. Ce mode de chiffrement est le plus simple mais il est très vulnérable aux attaques.

Le chiffrement : $C_i = E(m_i)$.

Pour le déchiffrement on inverse la fonction de codage:

Le déchiffrement est donné par : $m_i = D_k(C_i)$



Chapitre 3: Cryptographie moderne

Chiffrement Symétrique

Modes opératoires

Le mode Electronic Code Book (ECB)

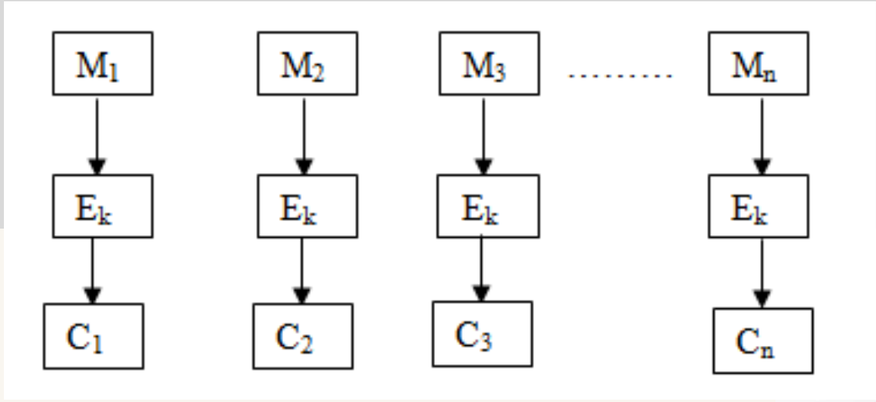
Dans ce mode, le message M est découpé en blocs mi de taille fixe.

Chaque bloc est alors chiffré séparément par une fonction, paramétrée par une clé k. Ainsi un bloc de message donné « m_i » sera toujours codé de la même manière. Ce mode de chiffrement est le plus simple mais il est très vulnérable aux attaques.

Le chiffrement : $C_i = E(m_i)$.

Pour le déchiffrement on inverse la fonction de codage:

Le déchiffrement est donné par : $m_i = D_k(C_i)$



Chapitre 3: Cryptographie moderne

Chiffrement Symétrique

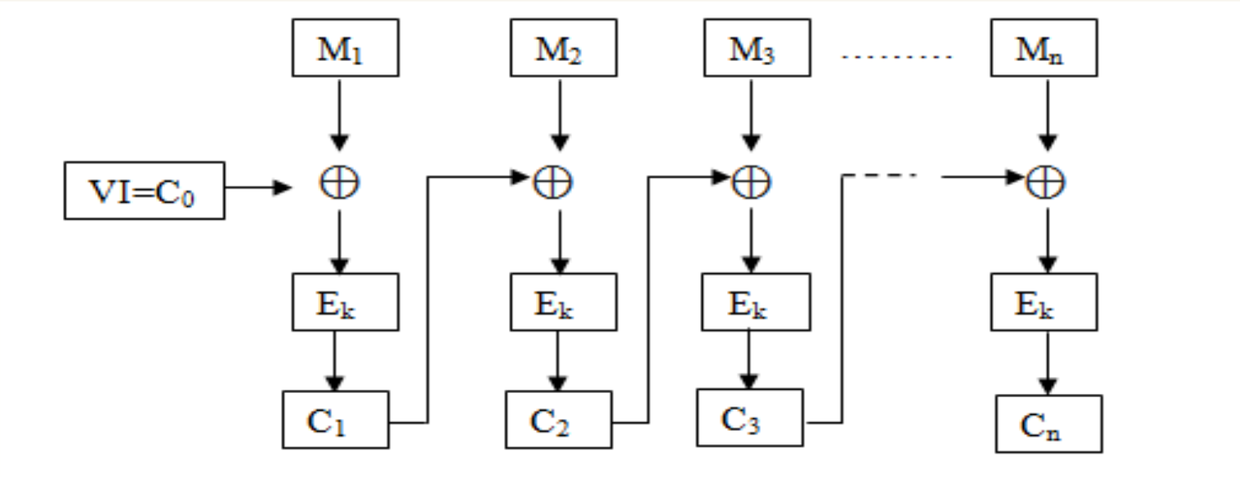
Modes opératoires

Le mode Cipher Block Chaining (CBC)

Le mode CBC a été introduit pour qu'un bloc ne soit pas codé de la même manière s'il est rencontré dans deux messages différents. Il faut ajouter une valeur initiale aléatoire (IV« Initial Value »).

Chaque bloc est d'abord modifié par XOR avec le bloc chiffré précédent avant d'être lui même chiffré. CBC est le mode de chiffrement le plus utilisé.

Le chiffrement : avec $C_i = E_k(m_i \oplus C_{i-1})$ avec $C_0 = 0$



Chapitre 3: Cryptographie moderne

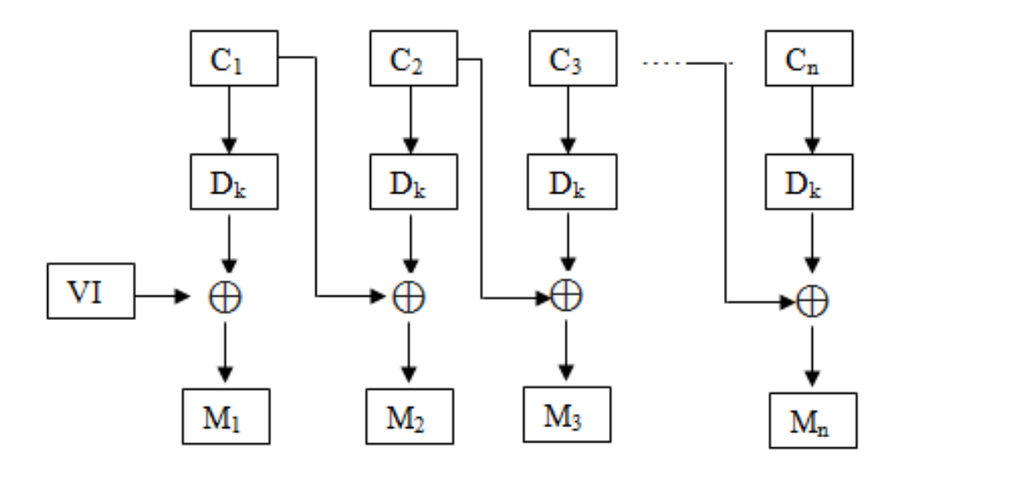
Chiffrement Symétrique

Modes opératoires

Le mode Cipher Block Chaining (CBC)

Le déchiffrement nécessite d'inverser la fonction de chiffrement : $D_K = E_K^{-1}$

$$m_i = C_{i-1} \oplus \mathrm{D_k}(C_i)$$



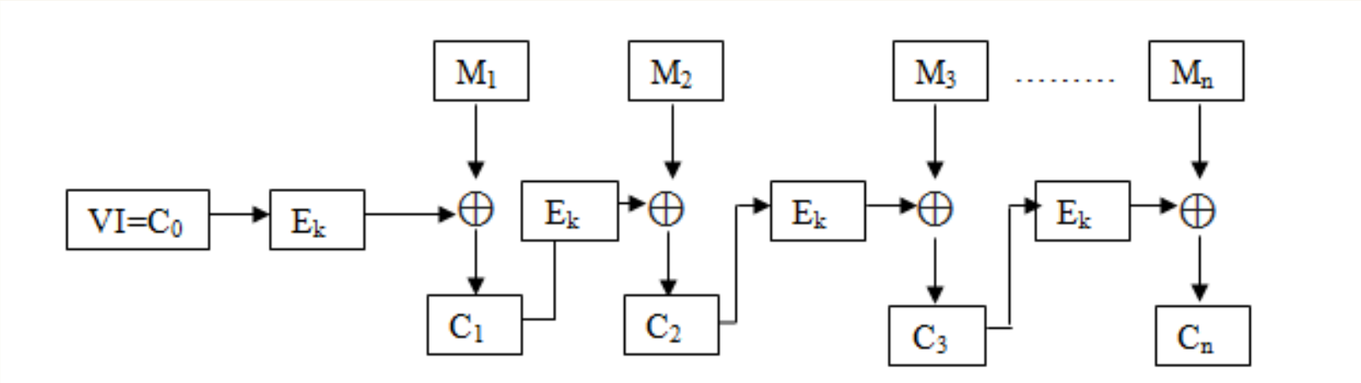
Chapitre 3: Cryptographie moderne

Chiffrement Symétrique

Modes opératoires

Le mode Cipher Feedback (CFB)

Dans ce mode le déchiffrement ne nécessite pas l'implémentation de la fonction inverse de la clé de chiffrement :
Le chiffrement est donné par : $C_i = M_i \oplus E_k(C_{i-1})$



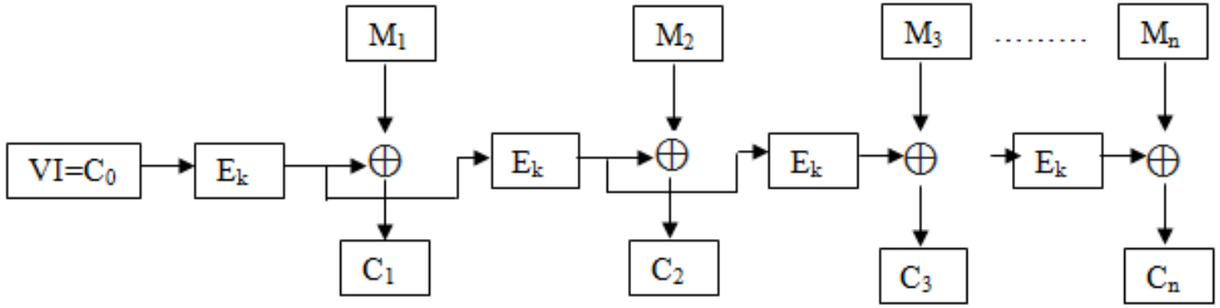
Chapitre 3: Cryptographie moderne

Chiffrement Symétrique

Modes opératoires

Le mode Output Feedback (OFB)

Le mode de chiffrement OFB est donné par : $C_i = M_i \oplus R_i$
Avec : $R_0 = C_0$, $R_i = E_k(R_{i-1})$
Le déchiffrement : $M_i = C_i \oplus R_i$, $R_i = E_k(R_{i-1})$

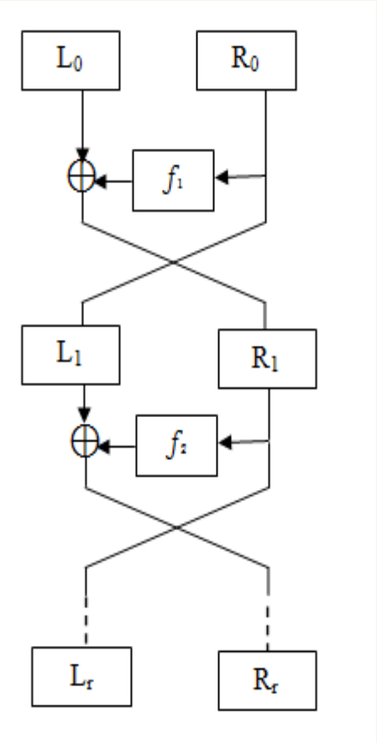


Chapitre 3: Cryptographie moderne

Chiffrement Symétrique

Schéma de Feistel

Un schéma de Feistel est un chiffrement itératif par blocs transformant $m = (L_0, R_0) \in F_2^m \times F_2^m$ en $C = (L_{r-1}, R_{r-1}) \in F_2^m \times F_2^m$
Par une procédure de $r \geq 1$ tours de Feistel.
Chaque tour transforme (L_{i-1}, R_{i-1}) en (L_i, R_i) utilisant une sous clé K_i et une fonction de confusion f par : $\begin{cases} L_i = R_{i-1} \\ R_i = L_{i-1} \oplus f(R_{i-1}, K_i) \end{cases}$
L'opération est inversible



Chapitre 3: Cryptographie moderne

Chiffrement Symétrique

Chiffrement DES et AES

DES (Data Encryption Standard)

- Algorithme développé par IBM dans les années 1970 (Lucifer) et adopter comme standard US par le NBS (FIPS 46-2), en 1977
- Taille de bloc = 64 bits
- Taille de Clé = 56 bits
- Schéma de Feistel à 16 tours

Chapitre 3: Cryptographie moderne

Chiffrement Symétrique

Chiffrement DES et AES

AES (Advenced Encryption Standard)

- Taille de bloc = 128 bits
- Taille de Clé = 128, 192, 256 bits

Structure générale

- Les données sont stockées dans un « carré » de 4 x 4 = 16 cases
- Chaque case contient 1 octet (8 x 16 = 128 bits d'état interne)

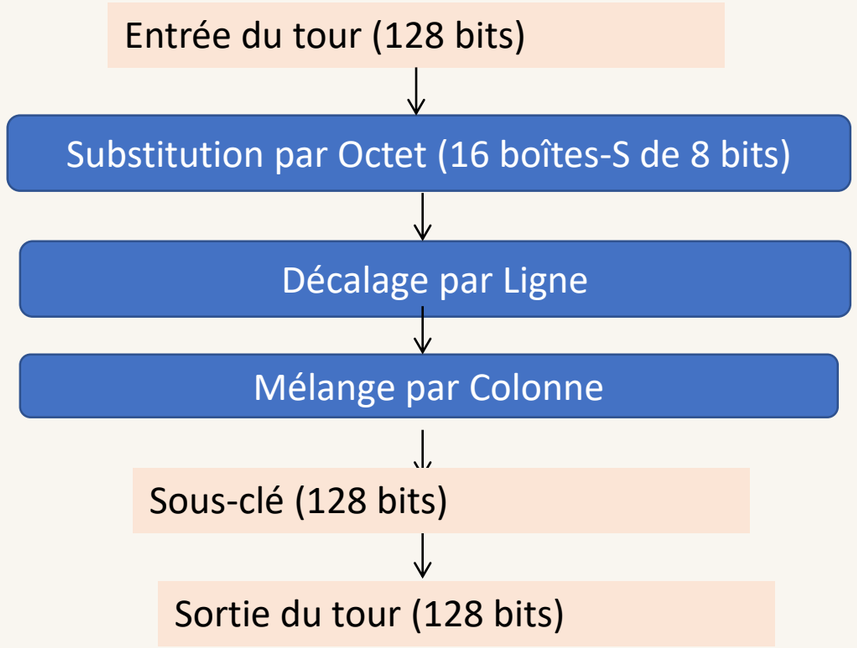
X1	X2	X3	X4
X5	X6	X7	X8
X9	X10	X11	X12
X13	X14	X15	X16

Chapitre 3: Cryptographie moderne

Chiffrement Symétrique

Chiffrement DES et AES

AES (Advenced Encryption Standard)
Fonction de tour



Chapitre 3: Cryptographie moderne

Chiffrement Symétrique

Conclusion

le chiffrement symétrique demeure l'une des méthodes les plus efficaces pour garantir la confidentialité des données, en raison de sa rapidité et de sa simplicité d'implémentation. Cependant, bien qu'il offre une sécurité solide lorsqu'il est utilisé avec des clés suffisamment longues et un algorithme robuste, il présente également des défis majeurs, notamment la gestion et la distribution sécurisée des clés. Les attaques potentielles, telles que celles basées sur l'analyse des clés ou les attaques par force brute, soulignent l'importance d'une clé secrète bien protégée. En dépit de ces défis, le chiffrement symétrique continue d’être une composante essentielle dans la protection des informations sensibles dans de nombreux systèmes de sécurité modernes.