Chapitre 02 : Cryptographie.

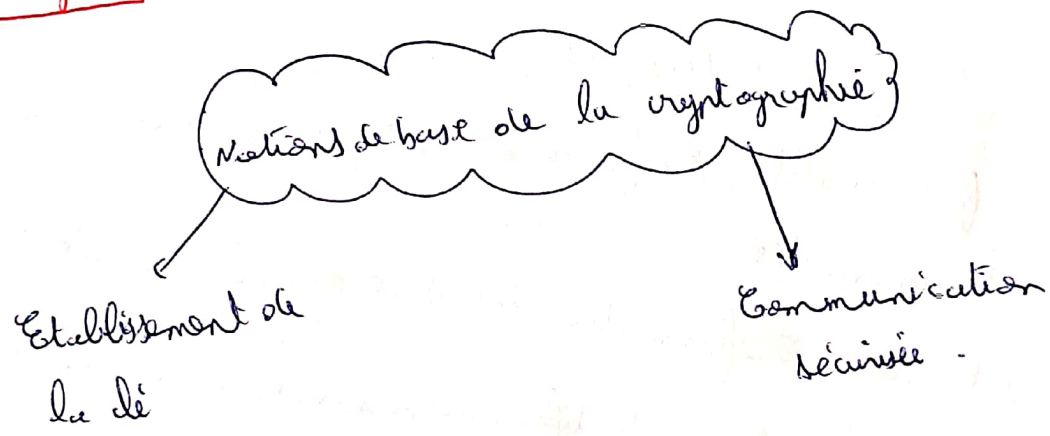
1)- Généralités et concept de base.

1)-1)- La cryptographie :

* Sécurité des communications
* Cryptage de fichiers sur disque
* Protection de contenu.
* Authentification des utilisateurs

1)-2)- Déf : Cryptographie :

- Art de concevoir des cryptosystèmes ; mécanisme assurant les services requis
- Cryptanalyse : Art de casser les cryptosystèmes.



1)-3)- Objectifs de la cryptographie :

Pour les attaques :

Scanné avec CamScanner

Passives :
- Espionnage

Actives :
- Usurpation d'identité
- altération des données
- répudiation des données : l'emetteur nié avoir envoyé le message
- destruction du message

1.4) Processus d'envoie de message :

Source :
- m : message
- $E(m) = c$ ← cryptogramme
  - E ← fonction de cryptage

Destination :
- m : message
- $D(c) = m$ ← message
  - D ← fonction de décryptage

1-5) Service de sécurité :

- **Confidentialité** : L'info ne doit pas parvenir à des personnes qui n'ont pas le la connaître.
- **Intégrité** : L'information ne doit pas subir d'altération
- **Authentification** : Identifier des personnes ou des entités et de certifier cette identité.
- **Non répudiation** : Enregistrer un acte ou un engagement d'une personne ou d'une entité de telle sorte qu'elle puisse ne pas nier ou avoir accompli cet acte ou pris cet engagement

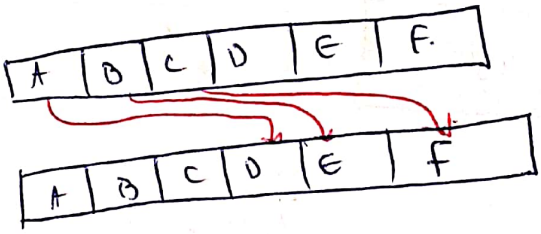
Scanné avec CamScanner

2) Historique de la cryptographie avant l'ère de la technologie.

2) - 1 - Le cryptogramme de César.

- Décalages circulant sur les lettres de l'alphabet.
- Décalage dans l'autre sens pour le déchiffrement.
- L'espace des clés : l'ensemble des décalages possibles
- Problème : sécurité faible, possible de tester toutes les clés à la main.

Exemple :



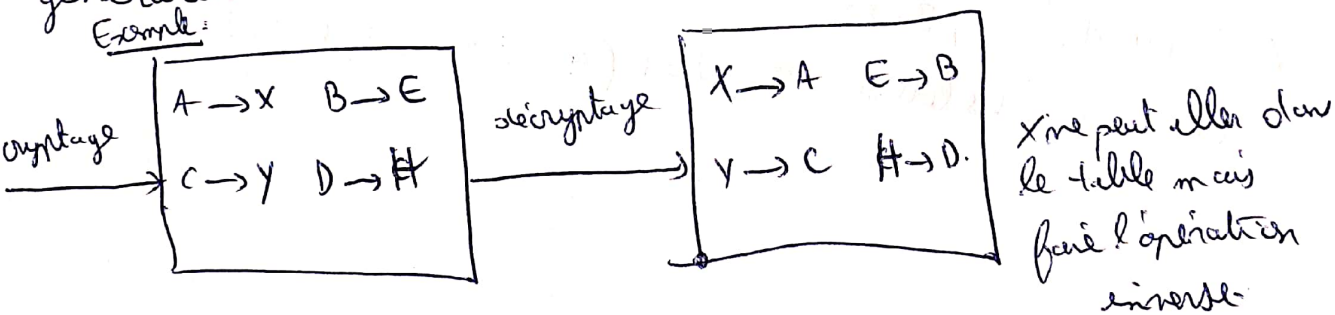
Attaque $\xrightarrow{\text{cryptage}}$ DWWDTXH.

DWWDTXH $\xrightarrow{\text{décryptage}}$ ATTAQUE.

2) - 2) - Le chiffrement par substitution.

- Association de chaque lettre de l'alphabet une autre lettre sans règle générale.

Exemple :



Avantage :
- Espace de clés est énorme (impossible de tester tout).

Inconvénients : - La clé est longue
- Sécurité faible

Scanné avec CamScanner

Exemple de calcul :

Si on prend l'exemple de l'alphabet :

- Pour crypter A : 26 choix.
  B : 25 choix.
  .....
- Nombre de clés = $26 \times 25 \times \dots \times 2 \times 1 = 26!$
  $= 4 \cdot 10^{26}$ clés

- Temps pour tester tout : avec une machine effectuant 1 000 000 clés/s

$$t = \frac{4 \cdot 10^{26}}{10^6} = 4 \cdot 10^{20} \text{ s} \approx 12 \text{ millions d'années}$$

Cryptanalyse de la substitution de lettres.

- Une même lettre est toujours crypter de la même façon.
- On se base sur la fréquence de lettres.

2)-3)- Le chiffrement de Vigenère :

- Correspondance lettre par des nombres.
  A = 0, B = 1, ..., Z = 25.
- Addition sur les lettres. J + W = F (9 + 22 mod 26 = 5)

Scanné avec CamScanner

2)-5)- Le différentiel de Hill :

- Correspondance lettre → nombre.

$A = 0$, $B = 1$, ..., $Z = 25$.

- La clé est représenté à l'aide d'une matrice.

$$\begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_n \end{pmatrix} \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1p} \\ \vdots & & & \\ a_{p1} & \cdots & \cdots & a_{pp} \end{pmatrix} \begin{pmatrix} \\ \\ \\ \end{pmatrix} \text{mod } 26 = \begin{pmatrix} C_1 \\ C_2 \\ \vdots \\ C_n \end{pmatrix}.$$

mat message — clé — cryptogramme.

Exemple :

$$\begin{pmatrix} m_1 \\ m_2 \end{pmatrix} \times \begin{pmatrix} a & c \\ b & d \end{pmatrix} = \begin{pmatrix} C_1 = a m_1 + m_2 \cdot b \\ C_2 = \end{pmatrix}$$

$m = \begin{pmatrix} 17 & 21 \\ 5 & 8 \end{pmatrix}$. $m = RE$.

$m = \begin{pmatrix} m_1 = 17 \\ m_2 = 4 \end{pmatrix}$

$$\begin{pmatrix} 17 & 4 \end{pmatrix} \begin{pmatrix} 3 & 21 \\ 5 & 8 \end{pmatrix} = \begin{pmatrix} 17 \times 3 + 4 \times 5 \\ \cdots \end{pmatrix} =$$

Scanné avec CamScanner

Exemple : clé = CRYPTO

N	O	U	S	A	T	T	A	Q	U	E	R	O	N	S	AU
C	R	Y	P	T	O	C	R	Y	P	T	O	C	R	Y	

$f((N + C) \bmod 26) = f((13 + 2) \bmod 26) = f(15 \bmod 26) = f(15) = .$

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V

22	23	24	25
W	X	Y	Z

2)-4) - Chiffrement de Vernan :

- Est un chiffrement de Vignère qui est sûr si et seulement si :

- La clé est aussi longue que le message.
- La clé n'est utilisée qu'une seule fois
- La clé est purement aléatoire.

Inconvenients :

- Echange de clé délicat
- Création difficile de la clée.
- Complexité de la gestion de la clé.

chiffré = message ⊕ clé

Message = chiffré ⊕ clé

Scanné avec CamScanner

Chiffrement symétrique

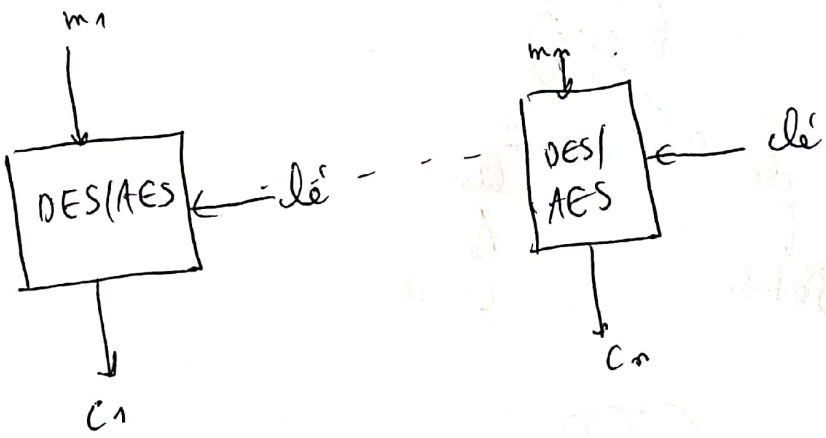
* Chiffrement par bloc :
  - DES : clé = 56 bits bloc = 64 bits
  - AES : clé = 128 bits bloc = 128 bits.

* Chiffrement par flot :
  - RC4 : chiffrement octet par octet.

1) - Chiffrement par bloc :

1) - 1) - Mode d'opération.

- Mode ECB.

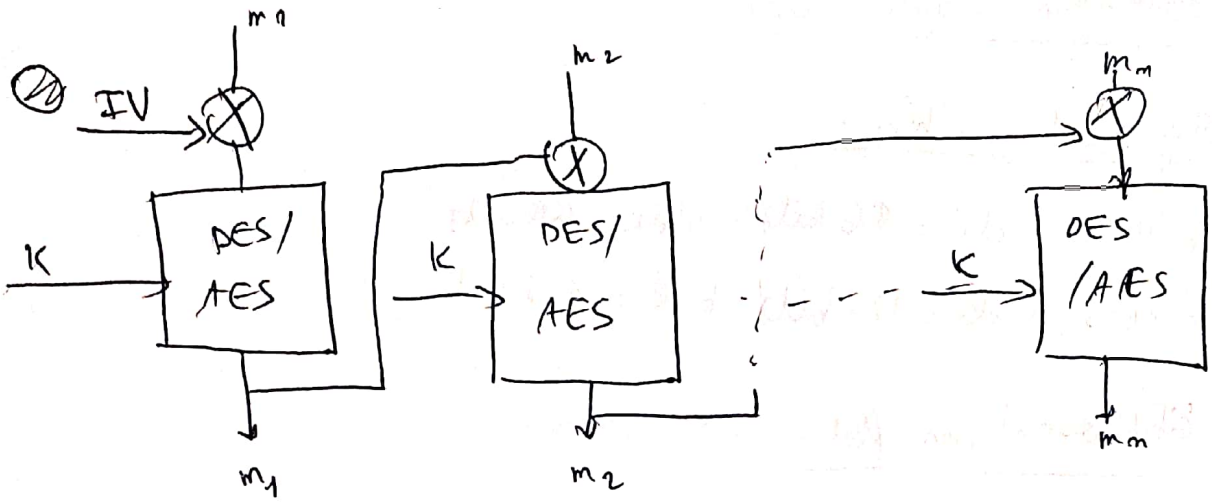


Avantage : - Simplicité
- Intégrité des blocs (indépendance des blocs)

Inconvénients : - Usure de la clé (expose le format des données)

Scanné avec CamScanner

Mode CBC :

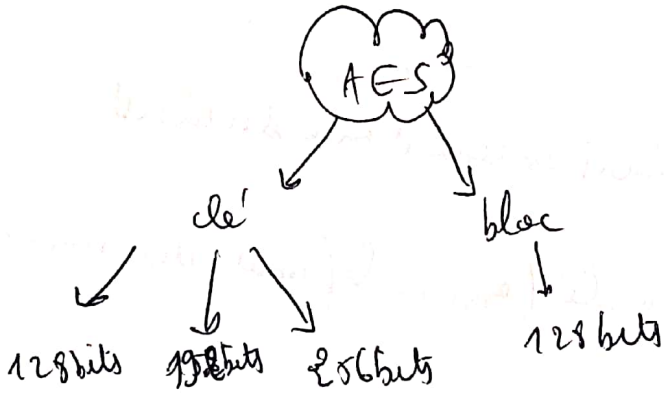


Avantage : Plus sur et presque aussi rapide que EBC.

Inconvenients : Si le bloc C_i est corrompu, alors on peut pas décoder

C_{i+1}.

Résumé :



Scanné avec CamScanner

• La perfection en cryptographie c'est l'aléatoire

* DES :

Algorithme à base de : - décalage
- « ou exclusif »
- transposition / rectangle

cryptanalyse de DES :

• Attaque par force brute.

Triple DES :

Appliquer 3 fois le protocole DES avec 3 clés différentes est considéré comme étant sûr.

AES :

nombre de rounds.

AES : 10 → clé 128
12 → clé 192
14 → clé 256

sans clé → 128 bits

Scanné avec CamScanner

La force d'un mot de passe :

- Un mot de passe est utilisé pour prouver l'identité : Authentification

La force d'un mot de passe : désigne sa capacité à résister à une énumération de tous les mots de passe possibles.

$$force = N^L$$

L : longueur du mot de passe

N : nombre de caractère.

Comment Estimer la force d'un mot de passe ?

- Comparaison avec les technique cryptographiques.
- Il est conseillé d'utiliser au minimum une clé de taille 100 bits
- AES → clé sur 128 bits

$$x = \frac{10 \cdot \ln(N)}{\ln(2)}$$

$$64^{10} = 2^x = \ln(64)^{10} = \ln(2)^x$$

$$10\ln(64) = x\ln(2)$$

$$\boxed{x = \frac{10 \cdot \ln(64)}{\ln(2)}}$$

Scanné avec CamScanner

Exemple :

1) – et 3h 50 s (QVD 3.

$N = 10 + 26 + 26 = 62.$

$L = 12$

$x = \frac{12 \ln(62)}{\ln(2)} = 71,45.$

• combinaisons possible = $3,22.10^{21}$ combinaisons.

Scanné avec CamScanner