Chapitre 1 : Généralités & Définitions

Plusieurs définitions de la sécurité informatique ou sécurité de l'information dans la littérature. Les plus pertinentes : (les mots clés sont soulignés)

- La **sécurité informatique** est l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaire et mis en place pour assurer la sécurité des systèmes informatiques.

1- Généralités & Définitions

- **Information security** is the practice of defending information from unauthorized access, use, revelation, disorder, modification, inspection, recording or destruction.

- La sécurité informatique c'est l'ensemble des moyens mis en œuvre pour minimiser la vulnérabilité d'un système contre des menaces accidentelles ou intentionnelles.

1- Généralités & Définitions

- **Menaces ou Risques accidentels**
- Incendie , Explosion, Inondation, tempête, Foudre,…
- **Vol et sabotage de matériels,** Destruction d'équipements, Destruction des supports de sauvegarde.
- **Autres risques liés** à l'organisation, à la gestion des personnels tels que : Départ de personnels stratégiques en retraite, maladies, décès,…, grèves

1- Généralités & Définitions

- **Les pannes et les erreurs (non intentionnelles)**
  - Pannes/dysfonctionnements du **matériel**.
  - Pannes/dysfonctionnements (Bug) du **logiciel de base, *Erreurs dans les applications***. (Bug 2000)
  - Oubli de sauvegarde, écrasement de fichiers erreur de saisie

1- Généralités & Définitions

- **Les menaces intentionnelles:**

- Détournement des données, l'écoute, les indiscrétions, Exemples: espionnage industriel espionnage commercial, Détournement des logiciels, copies illicites

- Attaques des logiciels (malveillantes à caractère informatique) **: V**irus, Ver, Spoofing (déguisement ou usurpation d'identité), Sniffing (écoute, analyse de trafic**,** espionnage d'une interface), Déni de service,…

1- Généralités & Définitions

- **Les méthodologies de sécurité**

- But: Identification et évaluation des risques ou des vulnérabilités (faiblesses) des systèmes d'information.

Réalisées par des grands utilisateurs de techniques de sécurité ou des groupes de travail, elles sont applicables par des prestataires de service sous forme d'audit de sécurité pour faire des propositions d'actions afin d'améliorer la situation

- Exemples de Méthodes :

- ✓ Méthode M.A.R.I.O.N (Méthode d'Analyse des Risques Informatiques et Optimisation par Niveau). Son Objectif est de mettre en place le schéma directeur de la sécurité des systèmes d'information SDSSI (méthode proposée en France à partir de 1984).
- ✓ Melisa (Méthode d'évaluation de la vulnérabilité résiduelle des systèmes d'information). France 1985

1- Généralités & Définitions

Exemples de Méthodes:

- ✓ Mehari (MEthode Harmonisée d'Analyse de RIsques) depuis 1995, elle est dérivée des méthodes Melisa et Marion.
- ✓ EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité). Méthode qui permet d'identifier les risques d'un SI et de proposer une politique de sécurité adaptée aux besoins de l'entreprise. C'est une méthode largement adoptée et publiée par la Direction centrale de la Sécurité des Systèmes d'information (France) en février 1997.
- ✓ Octave (Operationally Critical Threat, Asset, and Vulnerability Evaluation) a été créé aux Etats-Unis)en 1999.
- ✓ CCTA Risk Analysis and Management Method) a été inventée en Angleterre (1985)

1- Généralités & Définitions

- Pour être fiable, un système informatique doit être sécurisé.
- La fiabilité d'un système est définie comme la probabilité de son bon fonctionnement (sans défaillance) pendant une période de temps donnée, sous des conditions données.
- La fiabilité est indiquée par le MTBF (Mean Time Between Failures en anglais, ou Temps Moyen de Bon Fonctionnement avant Panne).
- Le MTBF s'exprime habituellement en nombre d'heures. Plus le MTBF est élevé, plus le système est fiable. Exemple: MTBF = 174805 heures (19,95 ans).

1- Généralités & Définitions

- **Objectifs et services de sécurité**

Ce sont les objectifs de base ou services de base qu'on tend à garantir pour assurer un fonctionnement sécurisé d'un système informatique.

Les principaux services ou objectifs à assurer sont en nombre de 05: Confidentialité, Authentification, Intégrité, Non répudiation, Disponibilité.

(Nous excluons la fiabilité de cet ensemble, car elle n'est pas un service de sécurité, mais un mode de fonctionnement nécessaire pour tous les services).

1- Généralités & Définitions

- **Confidentialité**

  Ce service assure que l'information soit inintelligible (incompréhensible, non déchiffrable) à des personnes autres que les acteurs de la communication.

- **L'authentification**

  Ce service s'assure de l'identité d'un utilisateur, seules les entités autorisées ont accès à l'information.

  Ce service est mis en place sur la base d'informations d'identification

  - ce qu'on sait (what we know) (identificateur et mot de passe)
  - ce qu'on a (what we have) (puce, carte magnétique, @réseau, …)
  - ce qu'on est (what we are) (emprunte digitale, iris, ADN, visage, voix,…)

1- Généralités & Définitions

- **Intégrité**

  Ce service doit assurer que les données n'ont pas été altérées (modifiées) durant la communication (de manière volontaire ou intentionnelle).

- **Non répudiation**

  Ce service doit assurer que l'auteur d'une action ne peut ensuite nier de l'avoir effectuée**.**

- **Disponibilité**

  Ce service doit assurer aux utilisateurs la continuité ou la pérennité de l'accès (à tout moment) à l'information.

1- Généralités & Définitions

- Les services de sécurité (authentification, confidentialité, non répudiation,…) utilisent des mécanismes essentiellement basés sur des techniques de cryptographie (utilisation de clés privées et /ou publiques pour le chiffrement et le déchiffrement ...)
- D'autres mécanismes sont utilisés pour la sécurité des réseaux (Firewall, VPN,…)

2- INTRODUCTION A LA CRYPTOGRAPHIE.

A- LEXIQUE ou VOCABULAIRE utilisé

- **Cryptographie** : C'est l'étude des méthodes et techniques servant à crypter du texte pour le protéger et assurer sa confidentialité, authenticité et intégrité en s'aidant de données *secrètes* ou clés.
- **Cryptanalyse** : Opposée à la cryptographie, elle a pour but de retrouver le texte clair à partir de textes chiffrés en déterminant les failles des algorithmes utilisés.
- **Cryptologie** : Il s'agit d'une science englobant deux branches : la cryptographie et la cryptanalyse

2- INTRODUCTION A LA CRYPTOGRAPHIE.

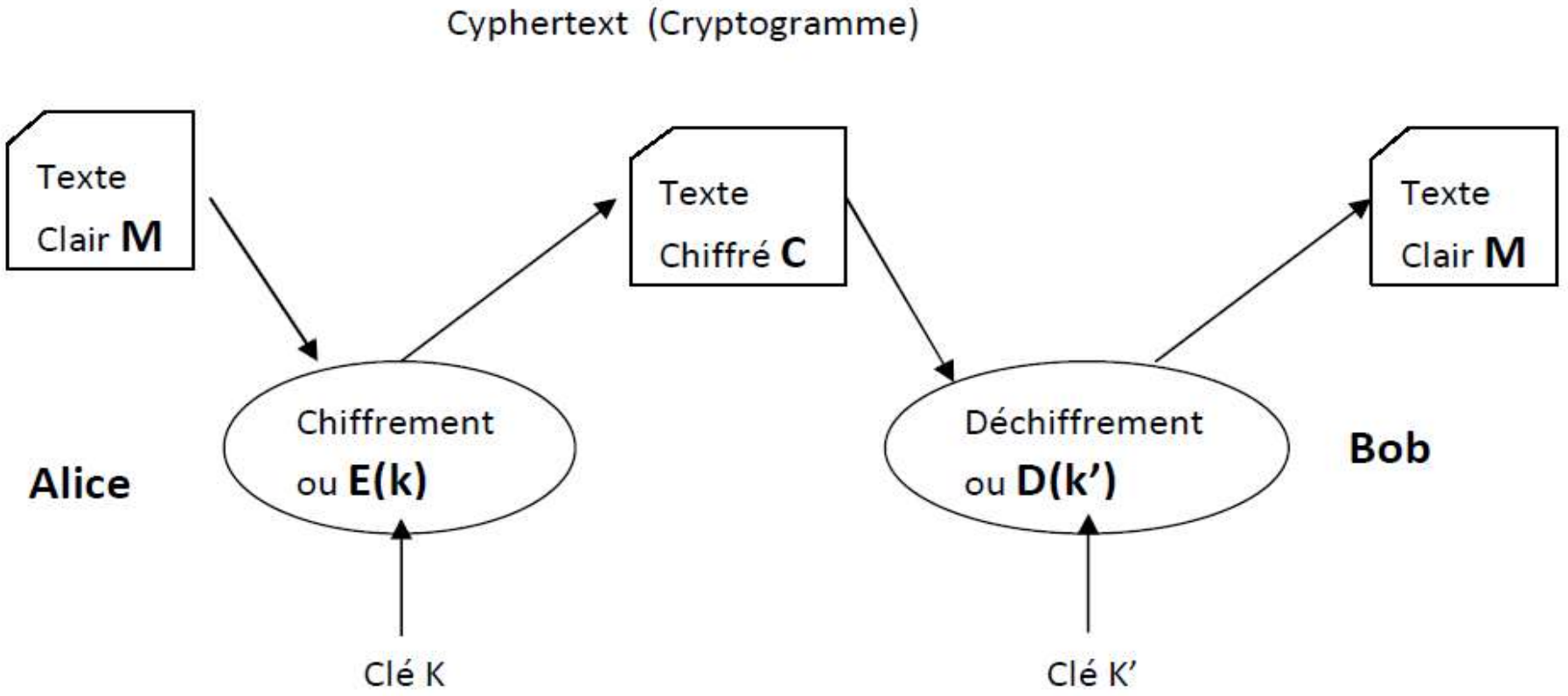
- **Chiffrement** : Le chiffrement consiste à transformer une donnée (texte, message, ...) afin de la rendre incompréhensible par une personne autre que celui qui a créé le message et celui qui en est le destinataire.
- **Déchiffrement:** La fonction permettant de retrouver le texte clair (plaintext en anglais) à partir du texte chiffré (cyphertext en anglais)
- **Texte chiffré :** Appelé également cryptogramme, le texte chiffré est le résultat de l'application d'un chiffrement à un texte clair.

2- INTRODUCTION A LA CRYPTOGRAPHIE.

- **Chiffre**: appelé aussi code secret, c'est en général, l'algorithme utilisé pour le chiffrement.
- **Clef** : Il s'agit du paramètre (suite de lettres ou de nombres) appliqué dans les différentes opérations de chiffrement et déchiffrement.
- **Crypto-système** : Il est défini comme l'ensemble des clés possibles (ensemble ou espace de clés), des textes clairs et chiffrés possibles associés à un chiffre (ou algorithme) donné.

2- INTRODUCTION A LA CRYPTOGRAPHIE

Notations et Conventions



2- INTRODUCTION A LA CRYPTOGRAPHIE

- Alice crypte (ou chiffre) le message M en exécutant la fonction (l'algorithme) de chiffrement E_k

$$M \xrightarrow{E_k} C=E_k(M) \text{ en utilisant la clé K.}$$

- Bob décrypte (ou déchiffre) le message chiffré C en utilisant la fonction (l'algorithme)de déchiffrement $D_{k'}$ utilisant la clé K'

$$C \xrightarrow{D_{k'}} D_{k'}(C)=D_{k'}(E_k(M))=M$$

où

- – M représente le texte clair, C est le texte chiffré
- – K clé de chiffrement, K' clé de déchiffrement

Remarque: Dépendamment du type de chiffrement (symétrique, asymétrique) les clés K et K' peuvent être les mêmes ou différentes

2- INTRODUCTION A LA CRYPTOGRAPHIE

- B- Differents types de Cryptographie

Il existe deux catégories essentielles de cryptographie moderne ou à usage général.

1- Symétrique (ou à clé secrète)

2- Asymétrique (ou à clé publique)

Une cryptographie dite classique a été utilisée anciennement, basée sur des techniques telles que la Substitution, la Permutation, la Transposition.

2- INTRODUCTION A LA CRYPTOGRAPHIE

- **1- CRYPTOGRAPHIE SYMETRIQUE**
  - **'CLASSIQUE'**

- **Par Substitution:** Chiffre de CESAR, Chiffre Affine

au message 'INFO': A=0,B=1, F=5, …I=8 …Z=25

la fonction f(x)=x+3 mod (26) correspondra le message 'MQJS'

- **Par Transposition** (ou Permutation)appliquée au message: ' UN TRES BON AMI EST UN TRESOR' donnera 'TO NO BIUSUSATRE ST RNE RN M E'

avec la permutation 4,3,1,6,5,2

1	2	3	4	5	6
U	N		T	R	E
S		B	O	N	
A	M	I		E	S
T		U	N		T
R	E	S	O	R	

2- INTRODUCTION A LA CRYPTOGRAPHIE

- **Cryptographie symétrique**
  - **‘moderne’**

- Par Blocs (de Taille fixe 64bits,128bits,…)
- Par Flots (à la volée)

Il existe différents modes opératoires de chiffrement par blocs

2. INTRODUCTION A LA CRYPTOGRAPHIE

Modes opératoires de Chiffrement

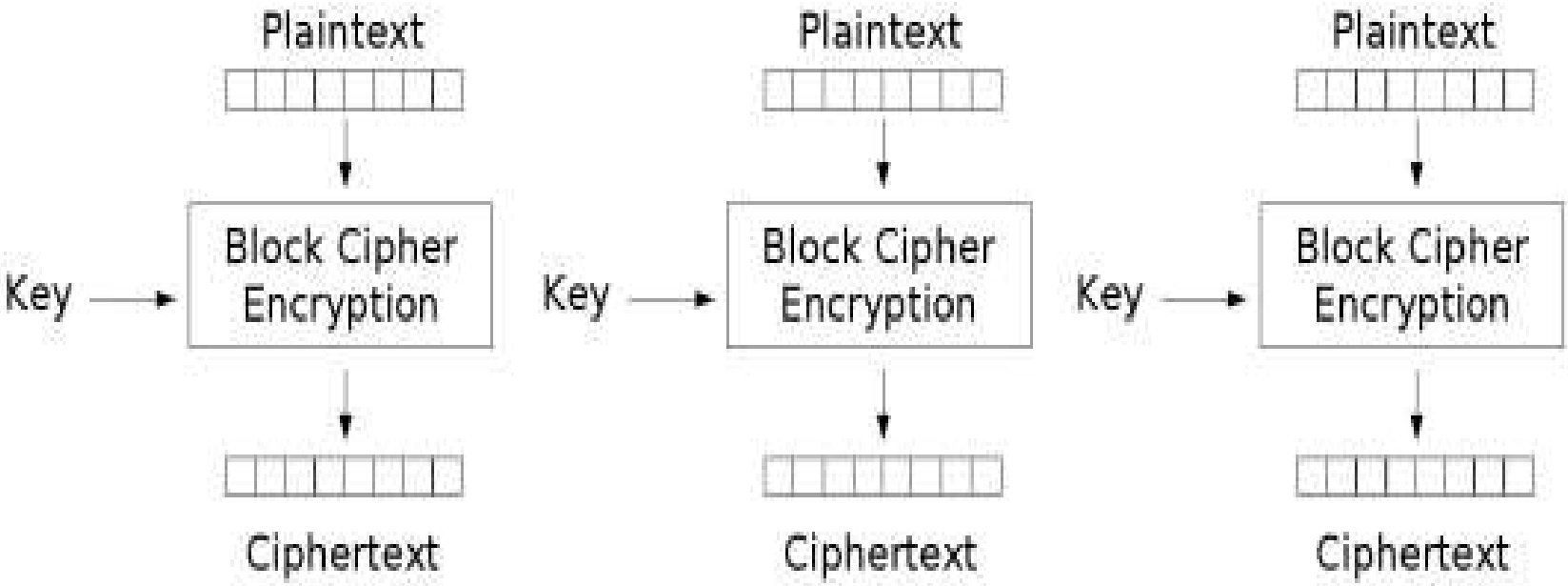
- Mode ECB (Electronic CodeBook).

Le mode le plus simple qui consiste à découper le message en blocs de n bits, et à appliquer la fonction de chiffrement à chacun de ces blocs avec la clé de chiffrement,

- Les blocs sont chiffrés indépendamment les uns des autres.
- Ce mode présente la faiblesse de produire toujours le même message chiffré avec le même message clair.

2. INTRODUCTION A LA CRYPTOGRAPHIE

Mode EBC (Electronic Codebook



Electronic Codebook (ECB) mode encryption

2. INTRODUCTION A LA CRYPTOGRAPHIE

- Mode CBC (Cipher Bloc Chaining)

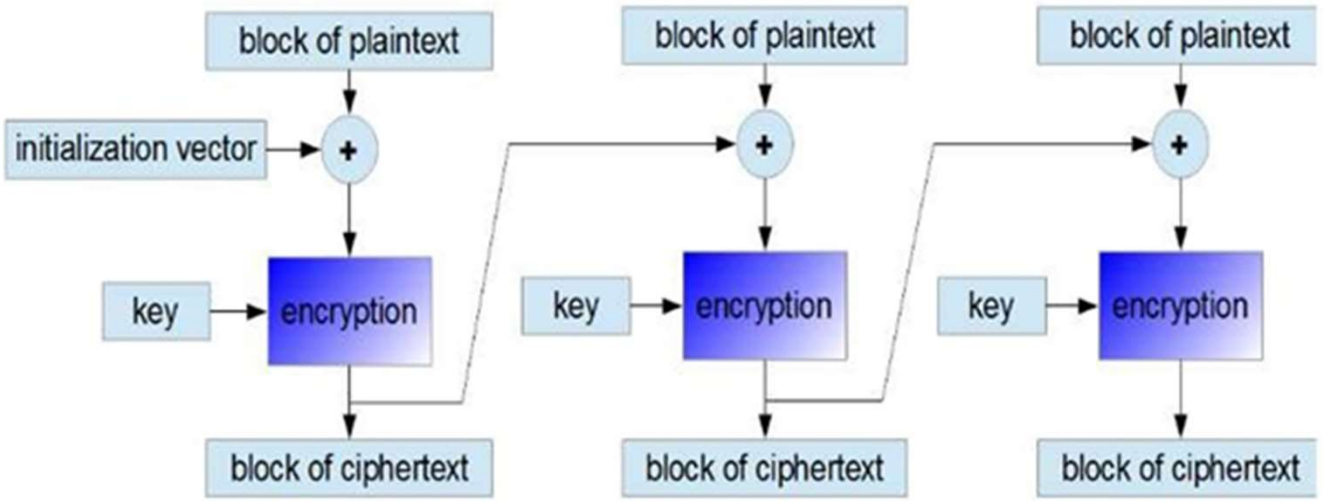
- Le mode de chiffrement très employé est le mode CBC (enchaînement des blocs). Il consiste à chiffrer le bloc i préalablement combiné avec par ou exclusif avec le bloc chiffré précédent, ainsi, **2 blocs en clair identiques d'un même fichier donneront des blocs chiffrés différents**.

- **ci = EK(mi ⊕ci−1)** pour tout i de 1 à t, avec:

  c0 = EK(m0 ⊕IV) où IV désigne un vecteur d'initialisation.

2- INTRODUCTION A LA CRYPTOGRAPHIE

- Mode CBC (Cipher Bloc Chaining)

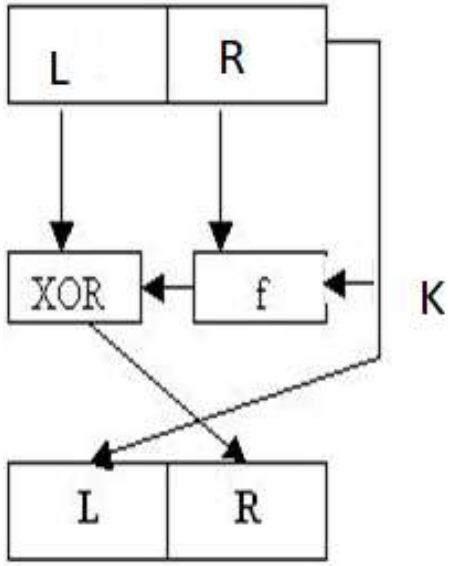


Cryptage en mode CBC

2- INTRODUCTION A LA CRYPTOGRAPHIE

- **Exemples de Cryptosystèmes symétriques** modernes:DES,3DES,AES

- **DES (Data Encryption Standard)** chiffrement par blocs, basé sur le modèle dit de Feistel
  - Dans le modèle de Feistel, le bloc est divisé en 2 parties : Gauche (Left) et Droite (Right)



  - Li+1=Ri d'où **Ri-1=Li** et Ri+1= Li Xor F(Ri,Ki)
  - d'où : Li-1=Ri Xor F(Ri-1,Ki)

2. INTRODUCTION A LA CRYPTOGRAPHIE

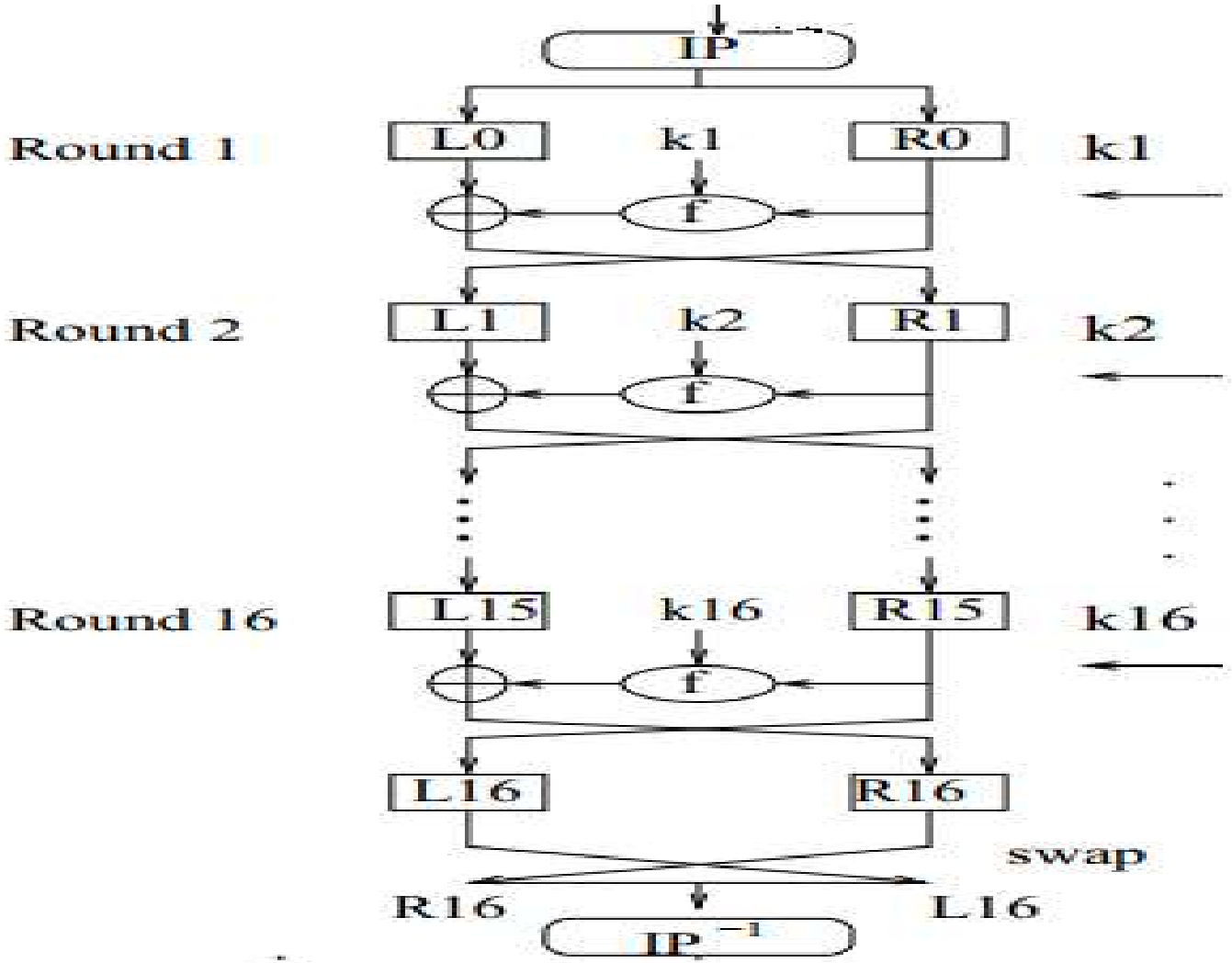
DES (Data Encryption System)

DES utilise des blocs de 64 bits (dont 8 bits de parité), le bloc est divisé en 2 parties : Gauche (Left) et Droite (Right) sur lesquelles sont exécutées des combinaisons d'opérations de substitutions et de permutations pendant répétées pendant 16 itérations (ou Rounds) après une permutation initiale des blocs , et à la fin on effectue une permutation inverse.

- F est une fonction produit combinant des substitutions et des permutations.

2. INTRODUCTION A LA CRYPTOGRAPHIE

DES (Data Encryption System)



2. INTRODUCTION A LA CRYPTOGRAPHIE

- Le **Triple DES**

Le Triple DES (ou 3DES) est un crypto système de chiffrement symétrique par blocs, enchaînant trois applications successives de l'algorithme DES sur le même bloc de données de 64 bits, avec des clés DES différentes.

- **AES Advanced Encryption System**

L'algorithme utilise en entrée un bloc de 128 bits (16 octets), et une clé de 128, 192 ou 256 bits selon la version.

- Le bloc de 16 octets en entrée est introduit sous forme de matrice 4x4 éléments (un octet/elt) pour subir différentes opérations (permutation, rotation, transformation linéaire).

- Ces différentes opérations sont répétées plusieurs fois « Rounds». Pour une clé de 128, 192 ou 256 bits AES nécessite respectivement 10, 12 ou 14 tours.

2- INTRODUCTION A LA CRYPTOGRAPHIE

Critique de la Cryptographie Symétrique

- Avantage : Rapidité, Ne nécessite pas une grande puissance de calcul
- Inconvénient: Problème de l'échange de la clé secrète. En général, on a recours à un chiffrement asymétrique (tel que Diffie-Hellman) pour l'échange de la clé secrète afin de l'utiliser pour crypter et décrypter un texte en utilisant un crypto système symétrique

2- INTRODUCTION A LA CRYPTOGRAPHIE

2- Cryptographie asymétrique (ou à clé publique)

. Basée sur la loi des grands nombres.

. Utilisation de deux clés:

- Une clé publique(publiée et partagée au préalable avec tout partenaire)
- Une clé privée gardée secrète par son propriétaire.

On note : Ksa (clé secrète d'Alice), Kpa (clé publique d'Alice), Ksb (clé secrète de Bob), Kpb (clé publique de Bob)

2- INTRODUCTION A LA CRYPTOGRAPHIE

La cryptographie (ou le chiffrement asymétrique) malgré qu'elle est considérée comme technique lourde et nécessitant souvent une grande puissance de calcul, peut être utilisée pour assurer **la confidentialité**, au même titre que le chiffrement symétrique

Dans ce cas:

Alice crypte (ou chiffre) le message M, à destination de Bob, en exécutant la fonction de chiffrement E_k

$$M \xrightarrow{E_{kpB}} C=E_{kpB}(M)$$

en utilisant la clé publique de Bob

- Bob décrypte (ou déchiffre) le message chiffré C en utilisant sa clé secrète K_{sB}

$$C \xrightarrow{D_{k'}} D_{k'}(C)=DK_{sB}(C)=M$$

2- INTRODUCTION A LA CRYPTOGRAPHIE

Autres Utilisations:

Signature Numérique

Fonction de Hachage

Au lieu de crypter tout le message, on utilise un condensé ou empreinte (un hash code) **de taille fixe** déduit du message de taille quelconque à signer grâce à une fonction de hachage (MD4 (Machine Digest, 1990) produisant un condensé de 128 bits,MD5,SHA1 (Secure Hash Algorithm,1995) produisant une empreinte de 160bits, SHA2, SHA3 avec des empreintes de tailles (224,256,384,512bits) selon la version.

La fonction de hachage est une fonction à sens unique: fonction mathématique facile à calculer mais dont la réciproque est coûteuse en temps de calcul.

2- INTRODUCTION A LA CRYPTOGRAPHIE

Signature Numérique

- Seule l'empreinte est cryptée en utilisant un chiffrement asymétrique.
- **Dans ce cas:**

Si E est l'empreinte déduite du message M après exécution de la fonction de hachage H alors E=H(M)

$$S_M = E_{Ksa}(H(M))$$

E_{ksa} est la fonction de chiffrement asymétrique de chiffrement utilisant la clé secrète d'Alice pour obtenir S_M la signature du message M.

Bob utilisera la clé publique d'Alice Kpa pour déchiffrer la signature du message et l'authentifier.

2- INTRODUCTION A LA CRYPTOGRAPHIE

- Signature Numérique

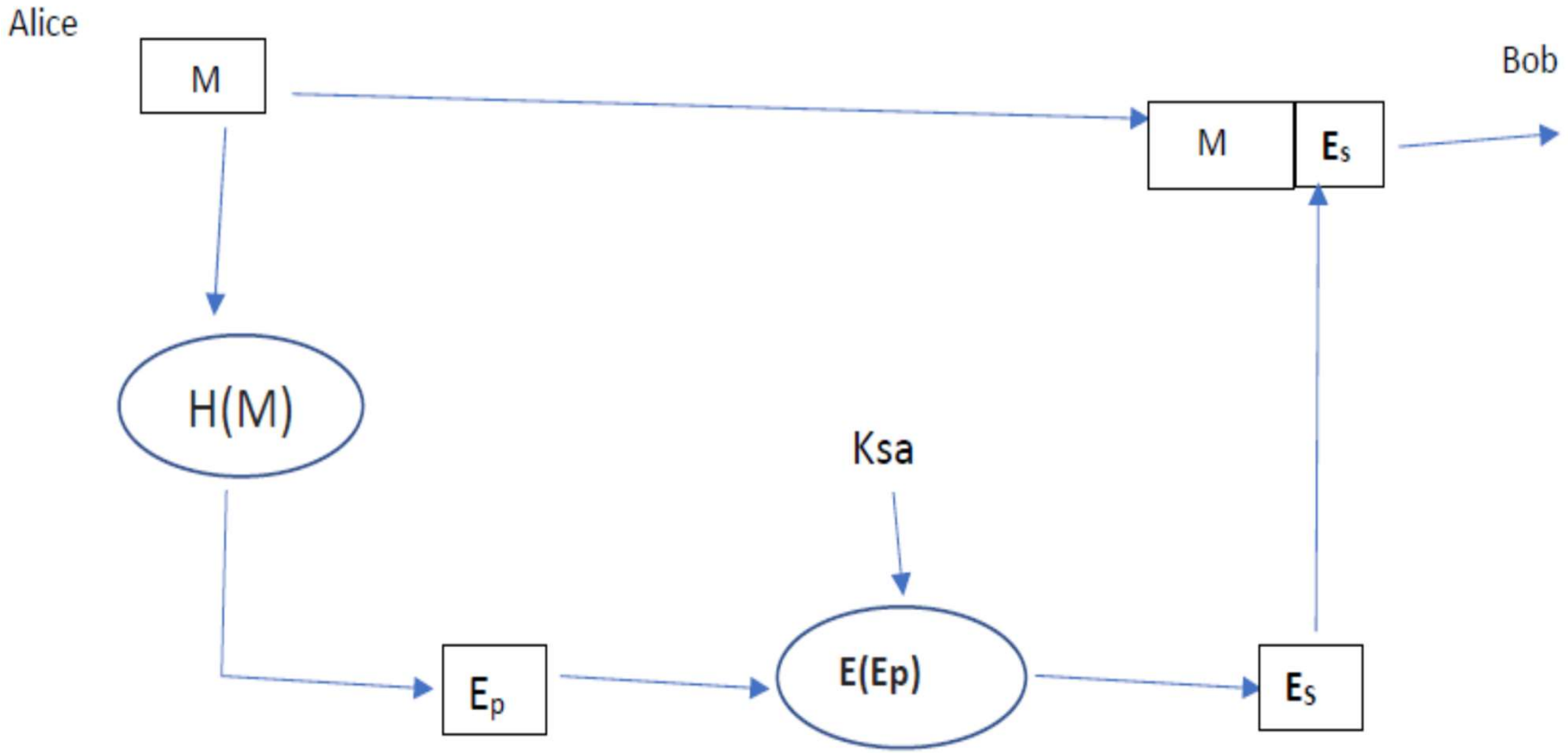
Alice crypte (ou chiffre) le message M en exécutant la fonction (l'algorithme) de chiffrement E_k

$$M \xrightarrow{E_{kSa}} C=E_{ksa}(E)$$

en utilisant sa clé privée

2- INTRODUCTION A LA CRYPTOGRAPHIE

Etape1 (chez Alice)

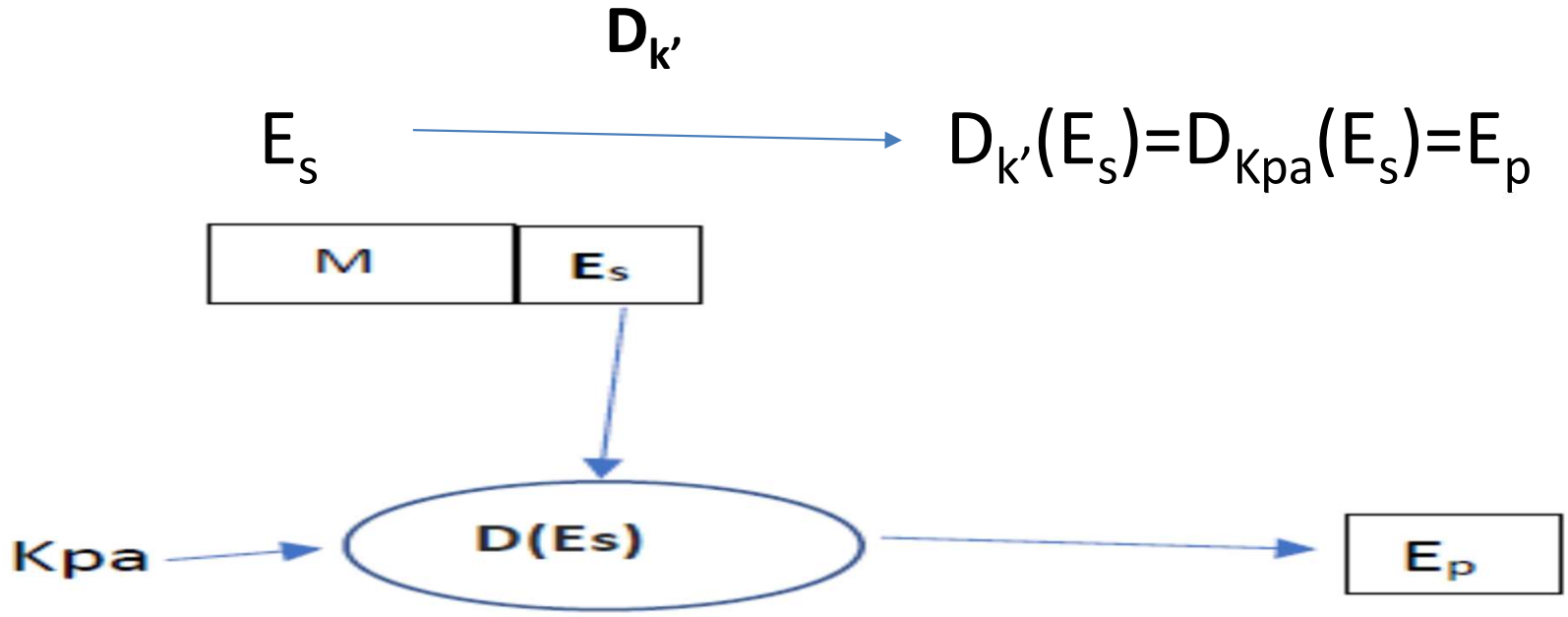


2- INTRODUCTION A LA CRYPTOGRAPHIE

Signature Numérique

Etape2 (chez Bob)

- Bob décrypte (ou déchiffre) le message chiffré C en utilisant la clé publique d'Alice



2- INTRODUCTION A LA CRYPTOGRAPHIE

Cryptographie Asymétrique

Autres Utilisations

- **Assurer l'Intégrité**

Bob s'assure de l'intégrité en exécutant la même fonction de hachage sur le message et la compare avec l'emprunte envoyée par Alice , après son déchiffrement en utilisant la clé publique d'Alice.

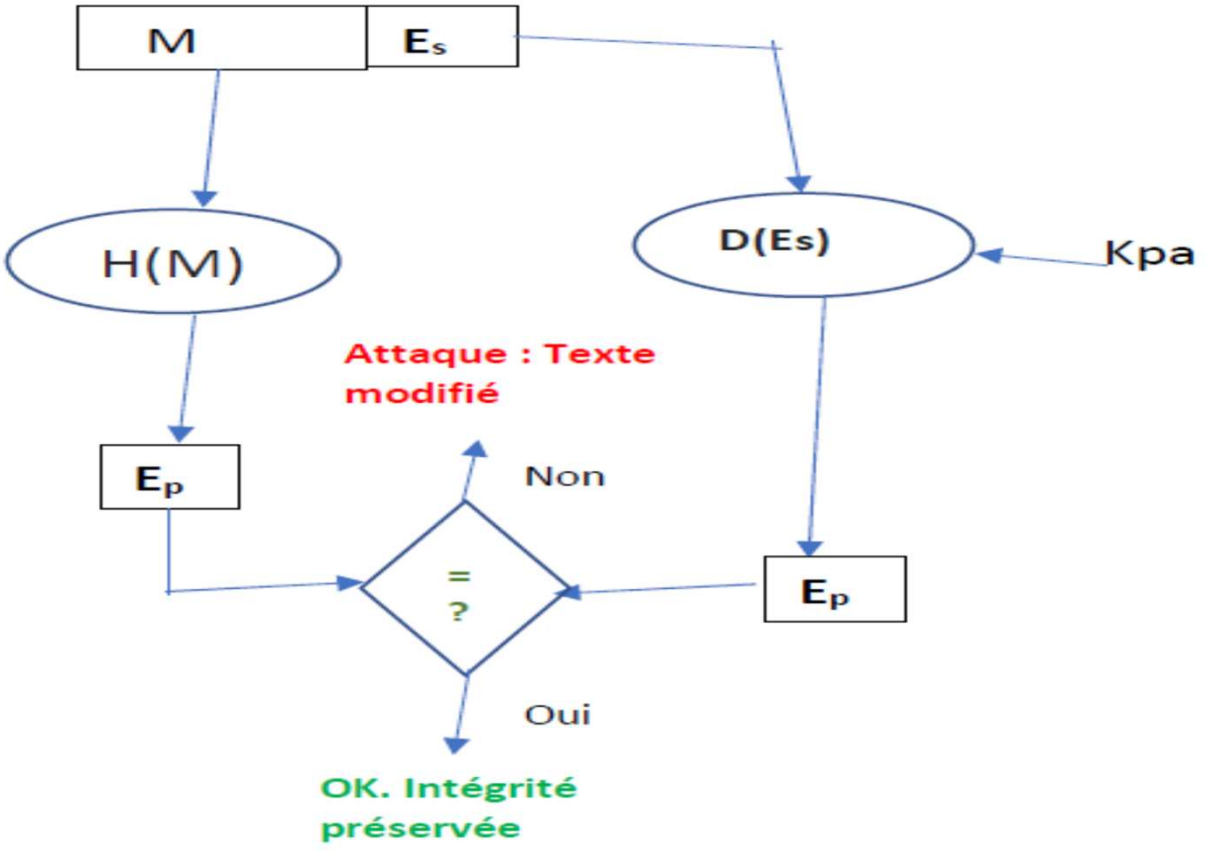
Si les deux empreintes sont égales alors on déduit que l'intégrité est préservée.

2- INTRODUCTION A LA CRYPTOGRAPHIE

Cryptographie Asymétrique

- Assurer l'Intégrité

Dans ce cas L'étape 2 au niveau de Bob devient :



2- INTRODUCTION A LA CRYPTOGRAPHIE

Autres Utilisations

Echange de la clé secrète: Diffie-Hellman

- Bob et Alice partagent une base g et un nombre premier p
- Alice choisit aléatoirement un nombre a et envoie à Bob la valeur: $g^a \bmod p$
- Bob choisit aléatoirement un nombre b et envoie à Alice la valeur: $g^b \bmod p$
- Alice calcule $(g^b \bmod p)^a \bmod p = g^{ba} \bmod p$
- Bob calcule $(g^a \bmod p)^b \bmod p = g^{ab} \bmod p = g^{ba} \bmod p$

La valeur (ou clé) secrète échangée est $g^{ab} \bmod p$

Ce protocole est basé sur la difficulté du problème du logarithme discret, c'est à dire pour retrouver à partir de g^a et b de g^b , est un problème que l'on ne sait pas résoudre,

2- INTRODUCTION A LA CRYPTOGRAPHIE

Exemple numérique:

- Bob et Alice partagent une base g=5, un nombre premier p=23
- Alice choisit a=6 et Bob choisit b=15 (aléatoirement)
- Alice envoie à Bob la valeur: $g^a \bmod p = 5^6 \bmod 23 = 8$
- Bob envoie à Alice la valeur: $g^b \bmod p = 5^{15} \bmod 23 = 19$

- Alice calcule $(g^b \bmod p)^a = 19^6 \bmod 23 = \underline{2}$
- Bob calcule $(g^a \bmod p)^b = (8^{15} \bmod 23) = \underline{2}$
- Clé secrète =2

2- INTRODUCTION A LA CRYPTOGRAPHIE

Cryptographie Asymétrique

- **Crypto-Système RSA**
- RSA est un crypto-système asymétrique inventé en 1977 par Ron Rivest, Adi Shamir et Leonard Adleman du MIT (Massachusetts Institute of Technology).
- De nombreux protocoles de sécurité sur Internet utilisent RSA pour leurs fonctions de chiffrement et de signature numérique.

2- INTRODUCTION A LA CRYPTOGRAPHIE

Cryptosystème **RSA**

- Le principe de RSA est basé sur l'utilisation de grands nombres premiers. Multiplier deux grands nombres est facile, mais déterminer les nombres entiers d'origine à partir du produit est considéré comme une opération très difficile et même impossible étant donné le temps qu'elle prendrait avec les ordinateurs actuels les plus puissants.

2- INTRODUCTION A LA CRYPTOGRAPHIE

L'Algorithme RSA (pour assurer la confidentialité)

- Choisir deux nombres premiers
- Calculer n appelé module de chiffrement n= p * q
- Calculer ϕ(n) appelé indice d'Euler ϕ(n) = (p - 1) * (q - 1)
- Choisir e exposant de chiffrement, premier avec ϕ(n), tel que 1 < e < ϕ(n)
- Calculer d tel que $d=e^{-1}$ mod(ϕ(n)) ou d*e= 1*mod(ϕ(n)).
- La clé Publique est (e, n)
- Le message chiffré du message M se calcule par:

$$C=M^{e} * Mod(n)$$

- La clé Privée est (d, n)
- Le message M obtenu à partir du message chiffré C est donné par :

$$M=C^{d} * Mod(n)$$

Cryptosystème **RSA**

- **L'Algorithme RSA (pour assurer l'authentification, signature numérique)**

- Le message chiffré du message M se calcule par:

$$C = M^d * \text{Mod}(n)$$

La clé Privée est (d, n)

- Le message M obtenu à partir du message chiffré C est donné par :

$$M = C^e * \text{Mod}(n)$$

La clé publique est (e, n)

TD

- Exercices

Le chiffre affine appliqué à l'alphabet affine est défini par la fonction : y=(ax+b) mod 26, avec une clé k=(a,b).

Pour une clé K=(1,3), ce chiffrement coïncide avec un autre chiffrement symétrique classique.

1-Quel est ce chiffre ?

2- Quel est le message crypté obtenu dans le cas du message clair 'INFO'?

3- A quelle condition la fonction de déchiffrement, inverse de la fonction affine

y=(ax+b) mod 26 peut-elle être définie ?

4- Le ROT (13) est un cas particulier du chiffre CESAR, Quelle est sa particularité?

5- Quel est le cryptogramme obtenu par le chiffre affine (a,b)=(5,4) ?

6-Donnez dans ce cas le message clair correspondant au cryptogramme 'QYOAL'

TD

- 7- Le masque jetable appelé aussi chiffre de Vernam ou encore ‘One Time Pad ‘ utilise une clé générée aléatoirement pour chaque message à chiffrer (l’ancienne clé est abandonnée). Le cyphertext est obtenu par un Oux (Ou exclusif) entre le texte et la clé. Ce crypto-système est pratiquement impossible à casser avec ‘la Brute force attack’ lorsqu’il s’agit d’une longueur de clé de 128 bits (et plus). Pourquoi?

8- Quelle est la différence entre un chiffrement poly alphabétique et un chiffrement monoalphabétique?

9- Chiffrer le message suivant à l’aide du chiffre de Vigenère avec la clef BONJOUR : ETUDIANTMASTERALUNIVERSITE

10- Donnez le message chiffré utilisant la transposition dans une matrice (m,n) avec m=4 , n=8) et le message (M= A^GOOD^^FRIEND^^IS^A^^^^TREASURE) ,0 le caractere ^ designe le blanc (ou espace), en utilisant la permutation K=(4,5,1,3,7,2,8,6).

11- Donner l’expression de la fonction de déchiffrement dans le modèle de Feistel appliquée à l’étage i-2.

12-Donnez le cipher text C correspondant au message M=8 en appliquant le crypto système RSA avec les deux nombres premiers p=3 et q=5, Vérifier que l’opération du déchiffrement donne le message M comme résultat.