Chapitre 1 : Introduction

M^me Abbaci Kahya Noudjoud

Objectifs de l’enseignement

- Ce cours a pour objectif de présenter à l’étudiant les bases de la cryptographie et ses différents algorithmes.

Motivations : les faits

- Chaque mois, 500 nouveaux virus et des variantes de virus sont découverts.
- Environ 60% des données résident sur des PC non protégé.
- 90% de sociétés et d'organismes gouvernementaux ont détectés des brèches de sécurité dans les systèmes informatique dans les derniers années.

Motivations : les effets

- Perte ou mise en danger de la vie humaine.
- Pertes financières.
- Déni de service.
- Utilisation ou abus non autorisée des systèmes informatiques.
- Perte, changement et/ou altération des données ou logiciels
- etc.

Qui est l'attaquant ?

Un adolescent

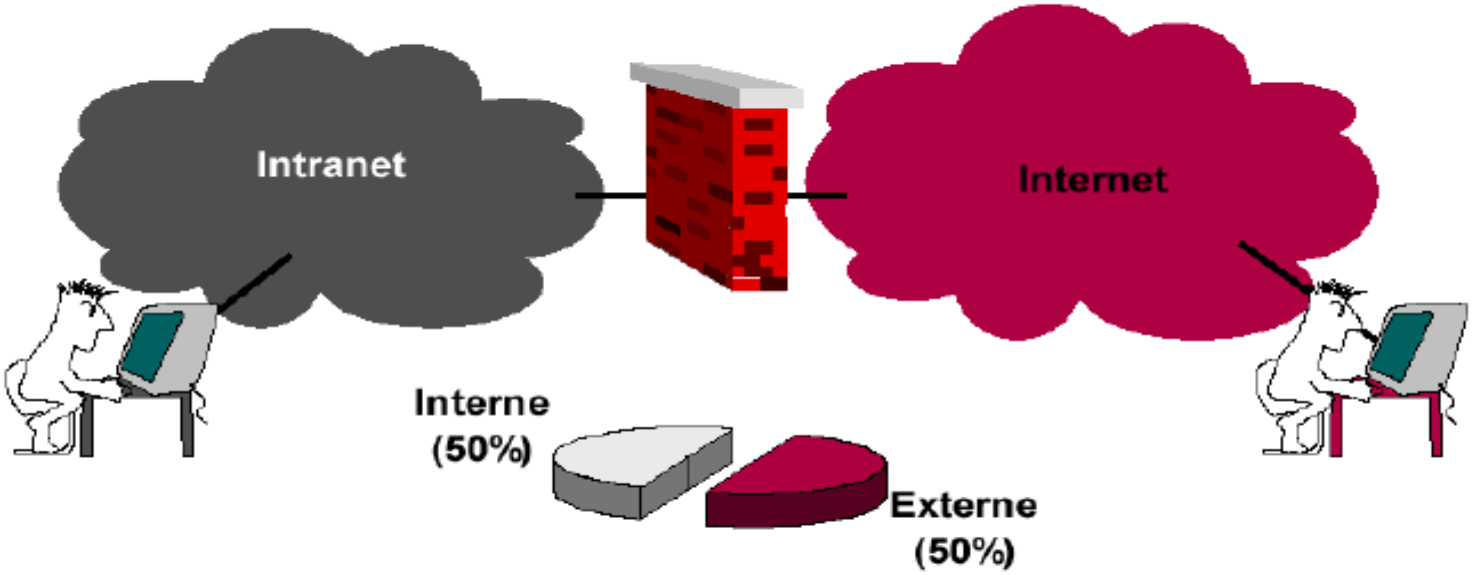
Un espion industriel

Un employé interne

Un gouvernement étranger

Un criminel

Externe Vs Interne



- Les attaques ne viennent pas seulement de l'extérieur!

Pourquoi attaquer ?

- Bénéfice et argent.
- Avantage concurrentiel.
- Revanche.
- Curiosité.
- Sottise.
- Attirer l'attention.

Où attaquer ?

- Les applications.
- Le support de communication
- La pile de protocoles.

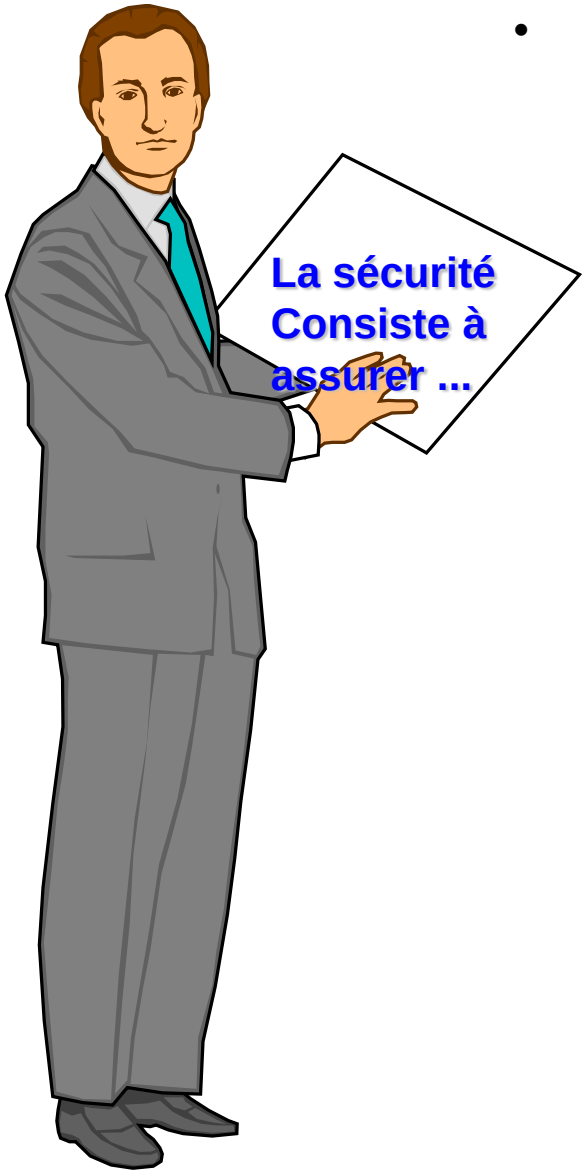
Quoi sécuriser ?

Le réseau « protocoles »

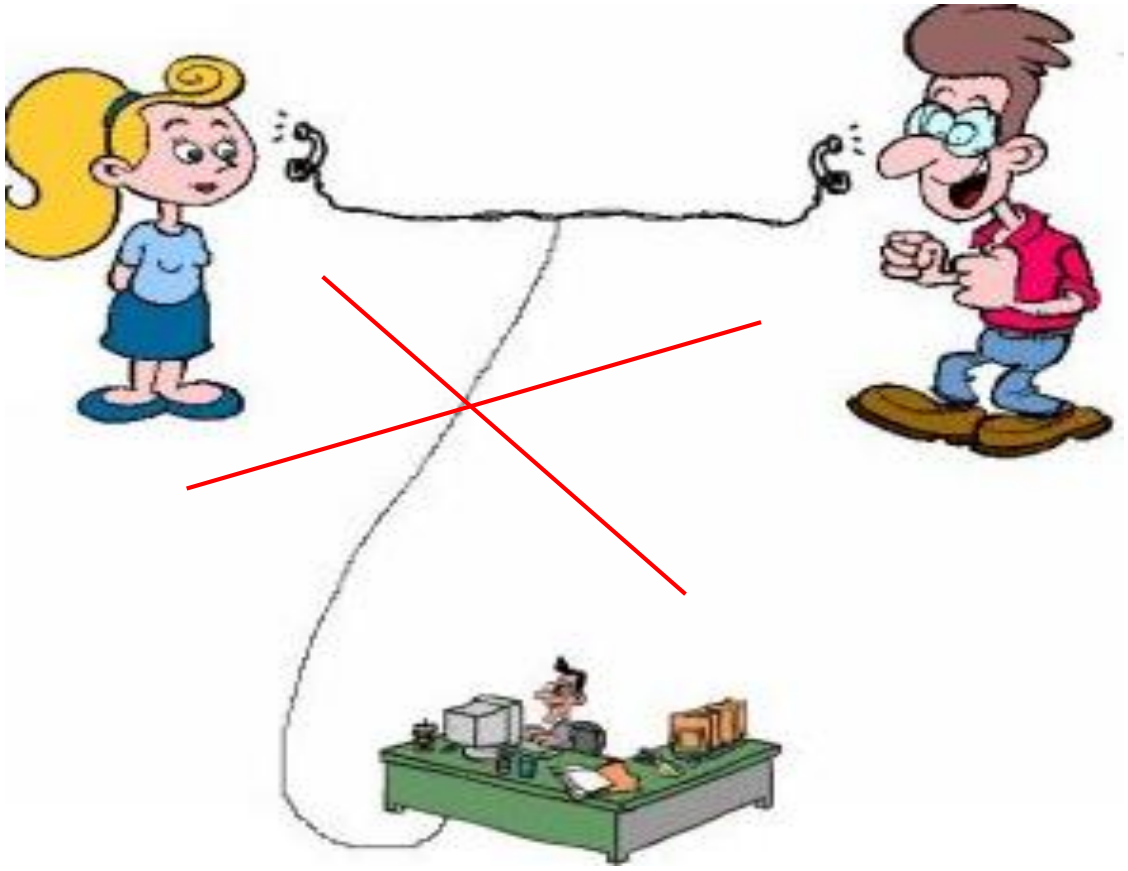
La machine
« applications et
Middleware»

Sécurité informatique

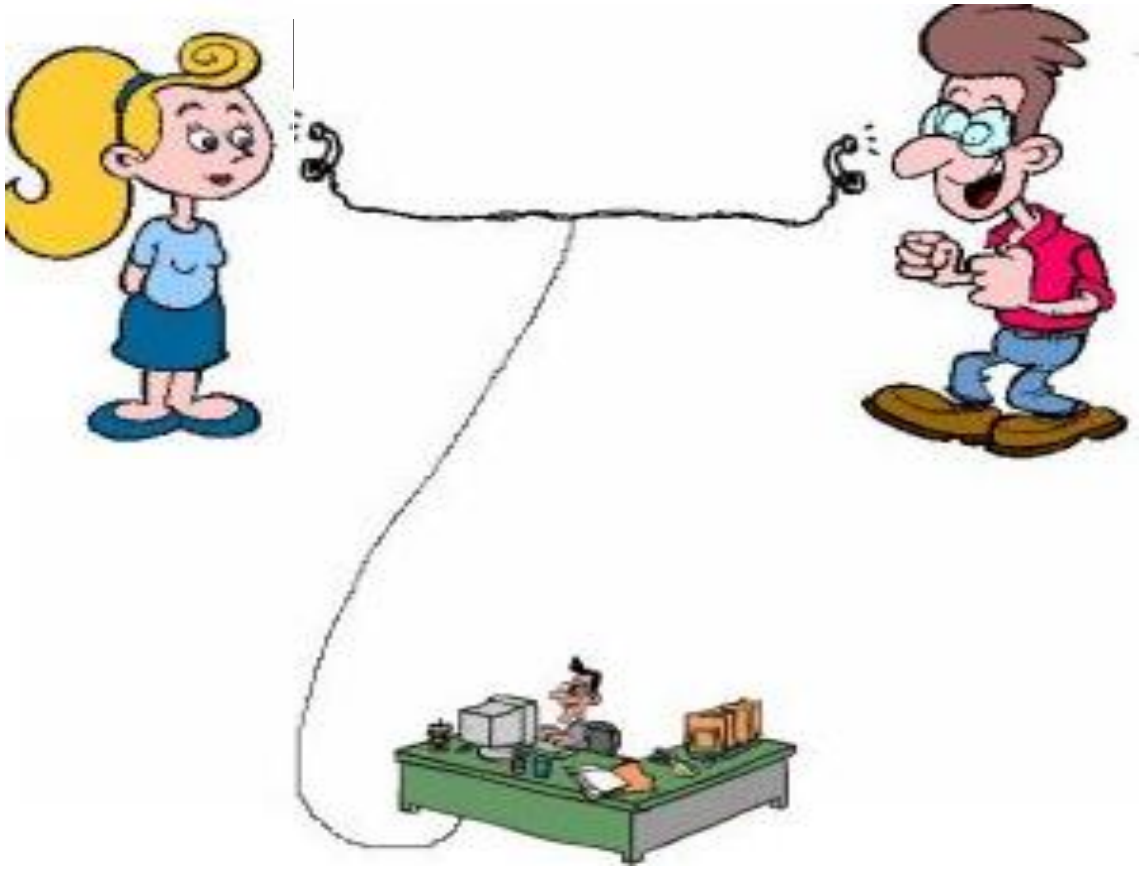
La sécurité informatique est l’ensemble de méthodes, techniques et outils mis en œuvre pour la protection des systèmes, des données et des services contre des menaces accidentelles ou intentionnelles afin d’assurer :



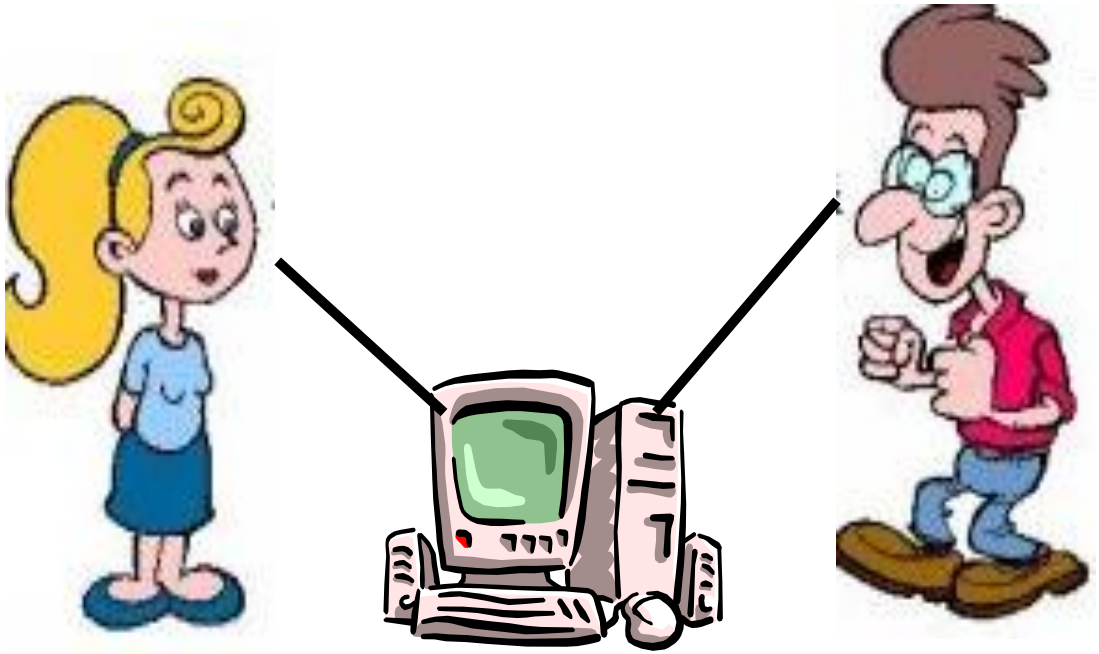
- **La confidentialité :** l'information échangée entre deux correspondants ne peut pas être consultée par un troisième.

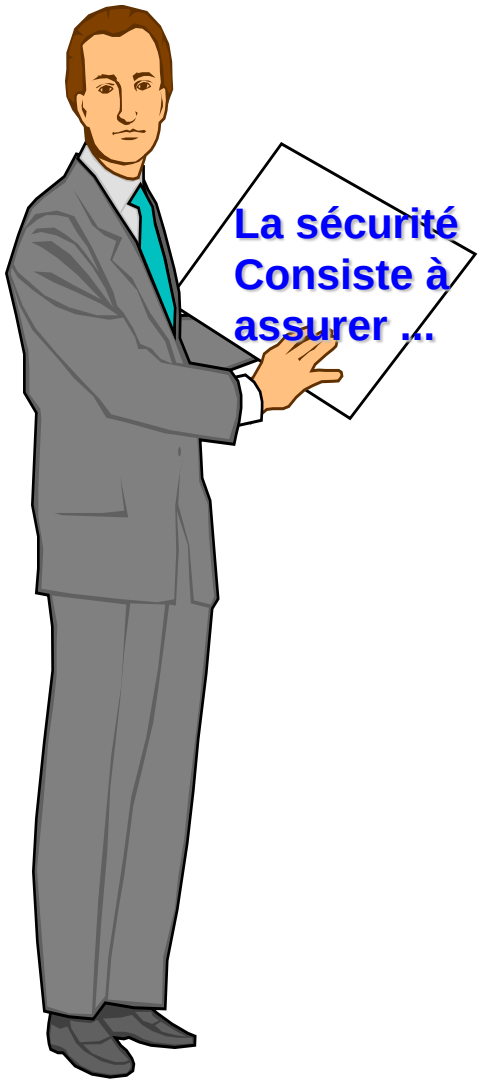


- **L'authentification :** les personnes utilisant une ressource correspondent aux noms d'utilisateurs.

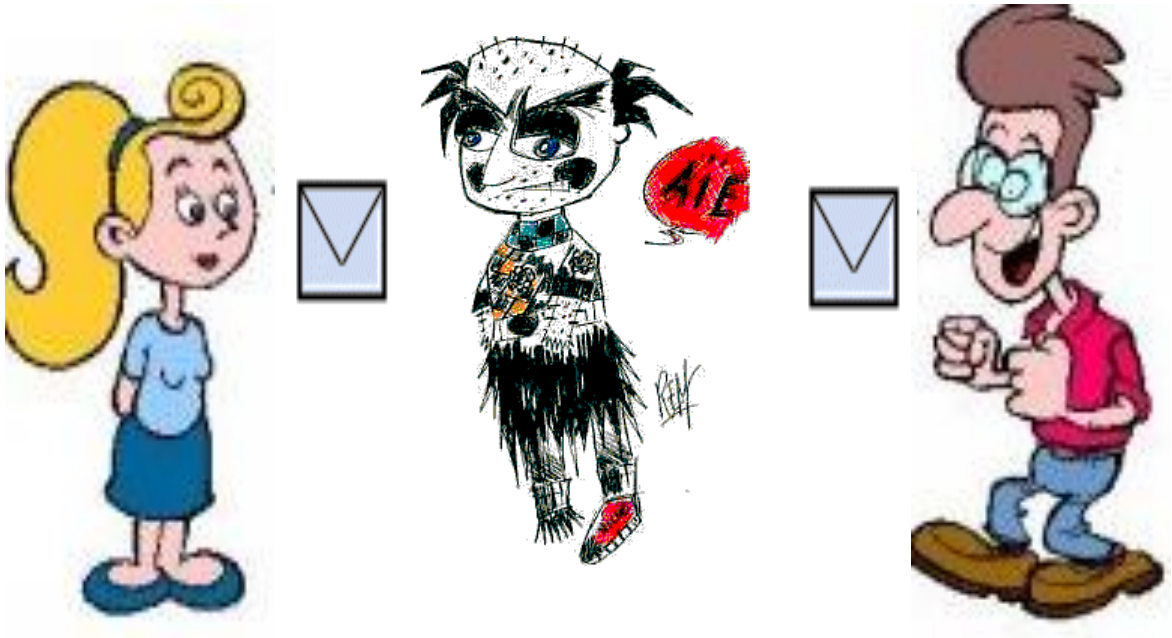


- **La disponibilité :** les données ainsi que les ressources du système informatique sont accessibles par ceux qui en ont besoin à chaque fois qu'ils demandent.





- **L'intégrité de données :** l'information n'est modifiée que par les personnes en ayant le droit, et de façon volontaire.



- **Non-répudiation:**

– **non-répudiation d'origine:** l'émetteur ne peut nier avoir écrit le message.

– **non-répudiation de réception:** le receveur ne peut nier avoir reçu le message.

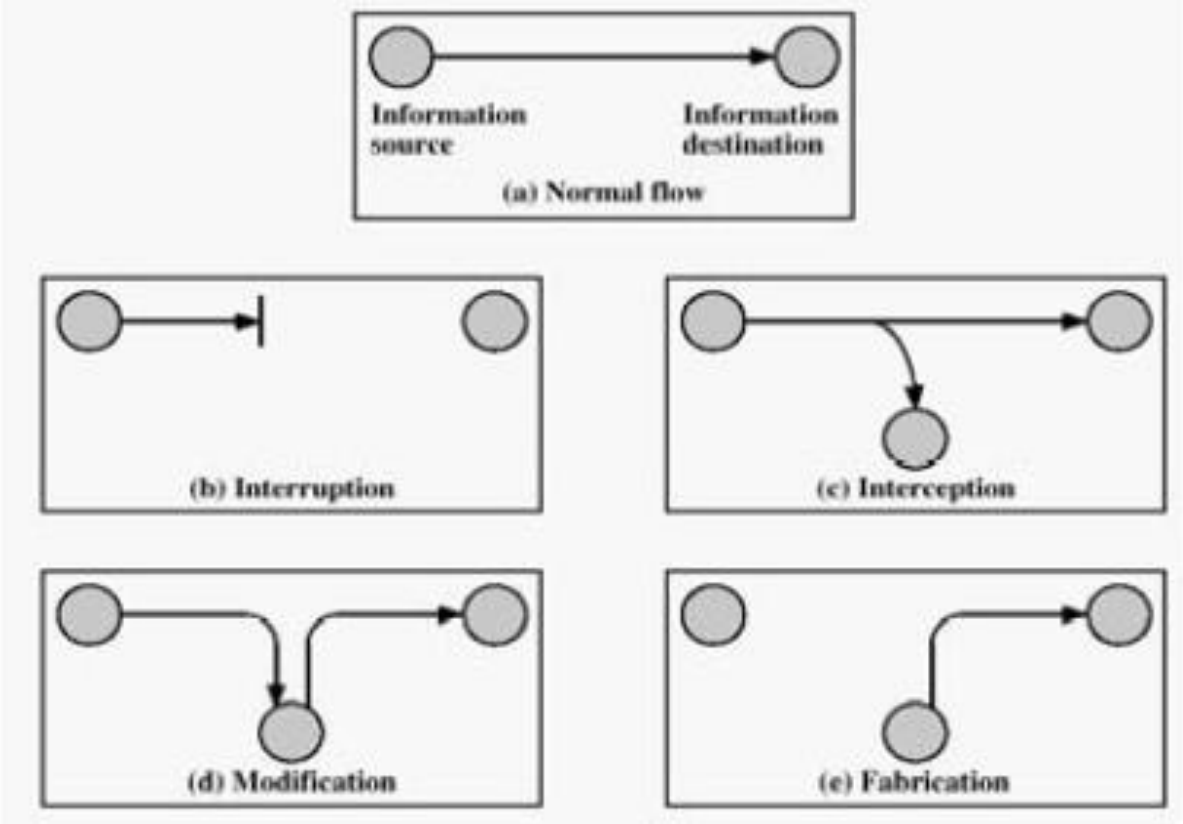
– **non-répudiation de transmission:** l'émetteur du message ne peut nier avoir envoyé le message.

Scénarios typiques

- Expéditeur et destinataire : deux entités importantes et reliées.
  Expéditeur (émetteur) →message→ destinataire (récepteur)

- intercepter + interrompre➔ Interruption : attaque sur la disponibilité
- intercepter + lire➔ Interception : attaque sur la confidentialité
- intercepter + modifier➔ Modification : attaque sur l'intégrité
- intercepter + fabriquer➔ Fabrication :attaque sur l'authenticité

Scénarios typiques



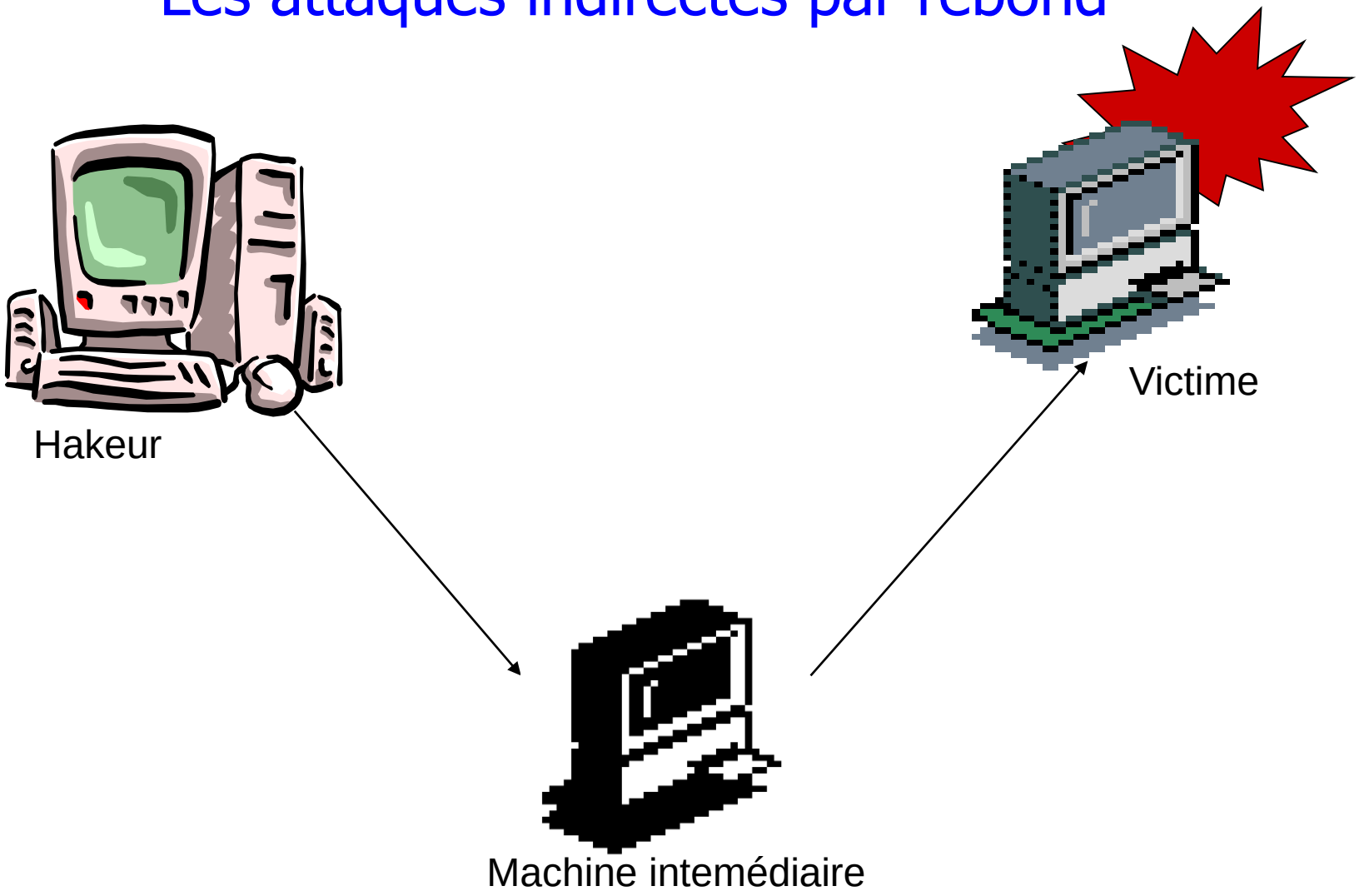

Les attaques informatiques

Les attaques directes

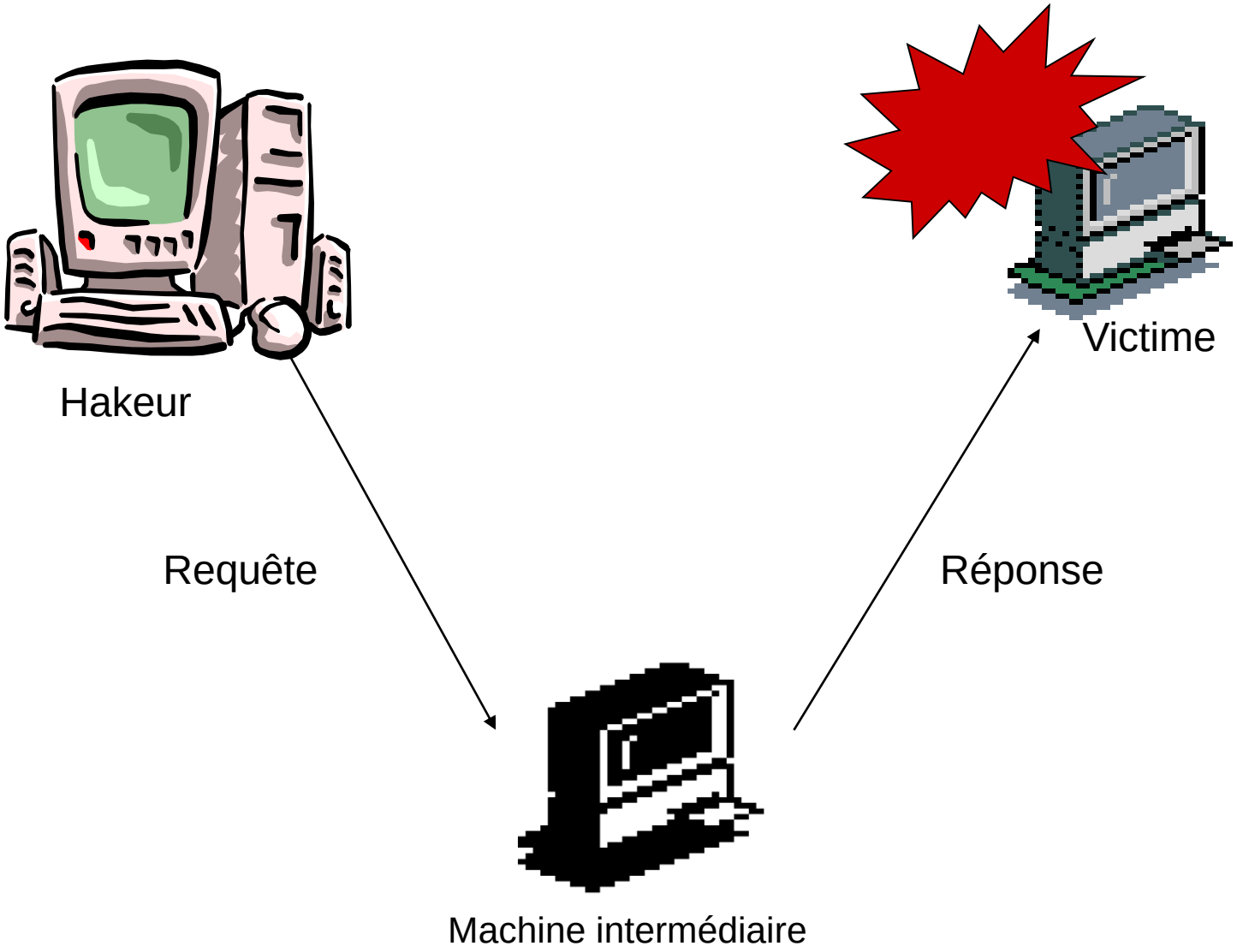
Hakeur

Victime

Les attaques indirectes par rebond



Les attaques indirectes par réponse



Types d'attaques

- Attaques sur les applications
- Attaques sur les protocoles de communication
- Attaques sur les protocoles de sécurité

Principales techniques de défense et de sécurité :

De nos jours différentes techniques et méthodes ont été développées pour mettre en œuvre une stratégie de sécurité :

- Authentification,
- Cryptographie,
- Firewalls,
- Proxy,
- VPN,
- Les anti-virus,
- Les systèmes de détection d'intrusion.

Concepts de base

- Un expéditeur Alice veut envoyer un message à un destinataire Bob en évitant les oreilles indiscrète d'Evé , et les attaques malveillantes de Martin.
- Pour cela Alice se met d'accord avec Bob sur le cryptosystème qu'ils vont utiliser. Ce choix n'a pas besoin d'être secret.

Concepts de base

- Alice veut être certaine
- qu'une personne non-autorisée (Eve) ne peut pas prendre connaissance de ses messages.
- que ses messages ne sont pas falsifiés par un attaquant malveillant (Martin)
- que le destinataire (Bob) a bien pris connaissance de ses messages et ne pourra pas nier l'avoir reçu (non-répudiation)

Concepts de base

- Bob veut être certain
- que le message reçu est authentique c'est à dire
  – que le message n'a pas été falsifié par un attaquant malveillant (Martin).
  – que le messages vient bien d'Alice (autrement dit qu'un attaquant (Oscar) ne se fait pas passer pour Alice, mascarade)
- que l'expéditeur (Alice) ne pourra pas nier avoir envoyé le message (non-répudiation)

Chapitre 2 : Cryptologie

Cryptographie

- La cryptographie est un ensemble de techniques qui protègent un message en le transformant en un autre message : cette transformation modifie l'information contenue dans le message original pour rendre l'information transmise non compréhensible.

- Les cryptographes inventent des méthodes de chiffrement de plus en plus complexes, composées d'une fonction de chiffrement et d'une fonction de déchiffrement.

Concepts de base

- Cryptographie : l'art et la science de garder le secret des messages.
  { secret (crypto) writing (graphy)}

- Cryptanalyse : l'art de décrypter les messages chiffrées.
  (Cryptanalistes = Codebreakers)

- Cryptologie : la branche des maths qui traite cryptographie + cryptanalyse.

- Texte en clair (M) : suite de bits, suite de caractères, voix numérisée, image vidéo digitale … transmis ou stocké.

- Texte chiffré (C) : information binaire - même taille que M - compressé - plus grande taille

Concepts de base

- La fonction de chiffrement est notée E (encryption)

$$E(M) = C$$

- La fonction de déchiffrement est notée D (decryption)

$$D(C) = D(E(M)) = M$$

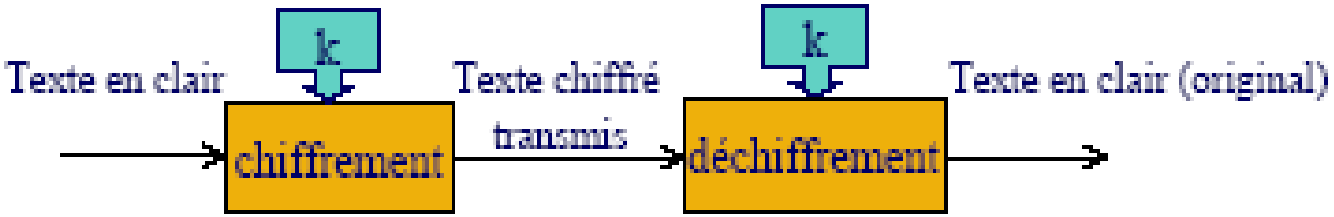
- Algorithmes cryptographiques : un algorithme cryptographique est une fonction math utilisée pour effectuer E et D.

- Il existe: - alg. de chiffrement de messages en clair
  - alg. de déchiffrement de messages chiffrés

Concepts de base

- Les algorithmes modernes de chiffrement utilisent une clé notée k.
- k prend un grand nombre de valeurs, espace des clés
- la clé de chiff = la clé de déchiff

$$E_k(M) = C \quad \Leftrightarrow \quad D_k(C) = D_k[E_k(M)] = M$$

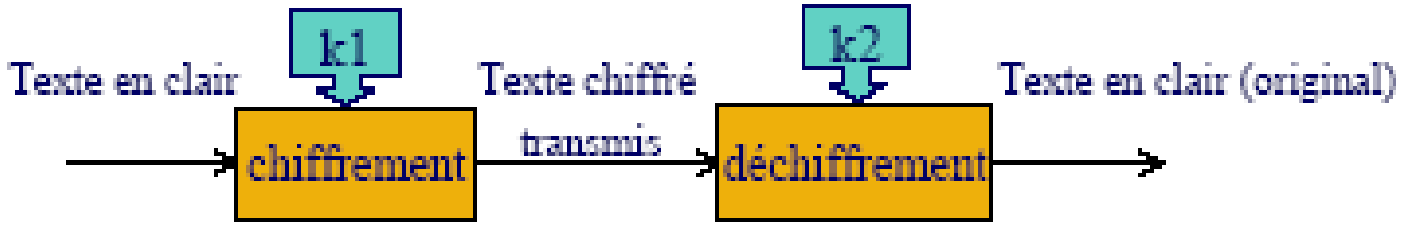


Chiffrement et déchiffrement avec une seule clé (symétrique)

Concepts de base

- Il existe des algorithmes où la clé de chiff =/= de la clé de déchiff dans ce cas :

$$\left.\begin{aligned} E_{K1}(M) &= C \\ D_{K2}(C) &= M \end{aligned}\right\} \quad D_{k2}[E_{k1}(M)] = M$$



Chiffrement et déchiffrement avec une deux clés (asymétrique)

Les clés symétriques

- Elles correspondent a des (mots de passe)
- La même clé est utilisée pour crypter et décrypter
- La clé doit être échangée

Les systèmes à clés asymétriques "publiques"

- Des clés différentes sont utilisées pour crypter et décrypter
- Les clés ont deux parties, l'une "publique", l'autre "privée"
- Seulement la partie "publique" des clés a besoin d'être changée

Exemple d’utilisation : clé symétrique

- Alice crypte un message avec une "clé"
- Elle envoie ce message crypté à Bob
- Bob décrypte le message . l’aide de la même clé
- Alice a donc dû transmettre la clé à Bob
- N’importe qui ayant la clé peut décrypter le message, la clé étant transmise, la sécurité est assez faible

Principe des systèmes à clés publiques

- On génère une paire de clés (l'une privée, L'autre publique) liées entre elles mathématiquement
- Les clés privées servent à décrypter les messages et doivent donc rester confidentielles
- Les clés publiques sont rendues publiques pour permettre d'encrypter un message.

- Bob a une paire de clés (privée + publique)
- Bob donne sa clé publique à Alice
- Alice crypte un message destiné à Bob en utilisant la clé publique de Bob, Alice sait que seul Bob (qui a la clé privée correspondante) pourra décrypter le message
- Bob décrypte le message à l'aide de sa clé privée.

Cours 3

Techniques cryptographiques classiques

Modèle de chiffrement conventionnel

Entité: Quelqu'un ou quelque chose qui envoie, reçoit ou modifie de l'information. Elle peut être une personne physique ou morale, un ordinateur, etc. Alice et Bob sont des entités.

Expéditeur: Entité qui envoie légitimement de l'information dans une transmission à deux parties. Alice est l'expéditrice.

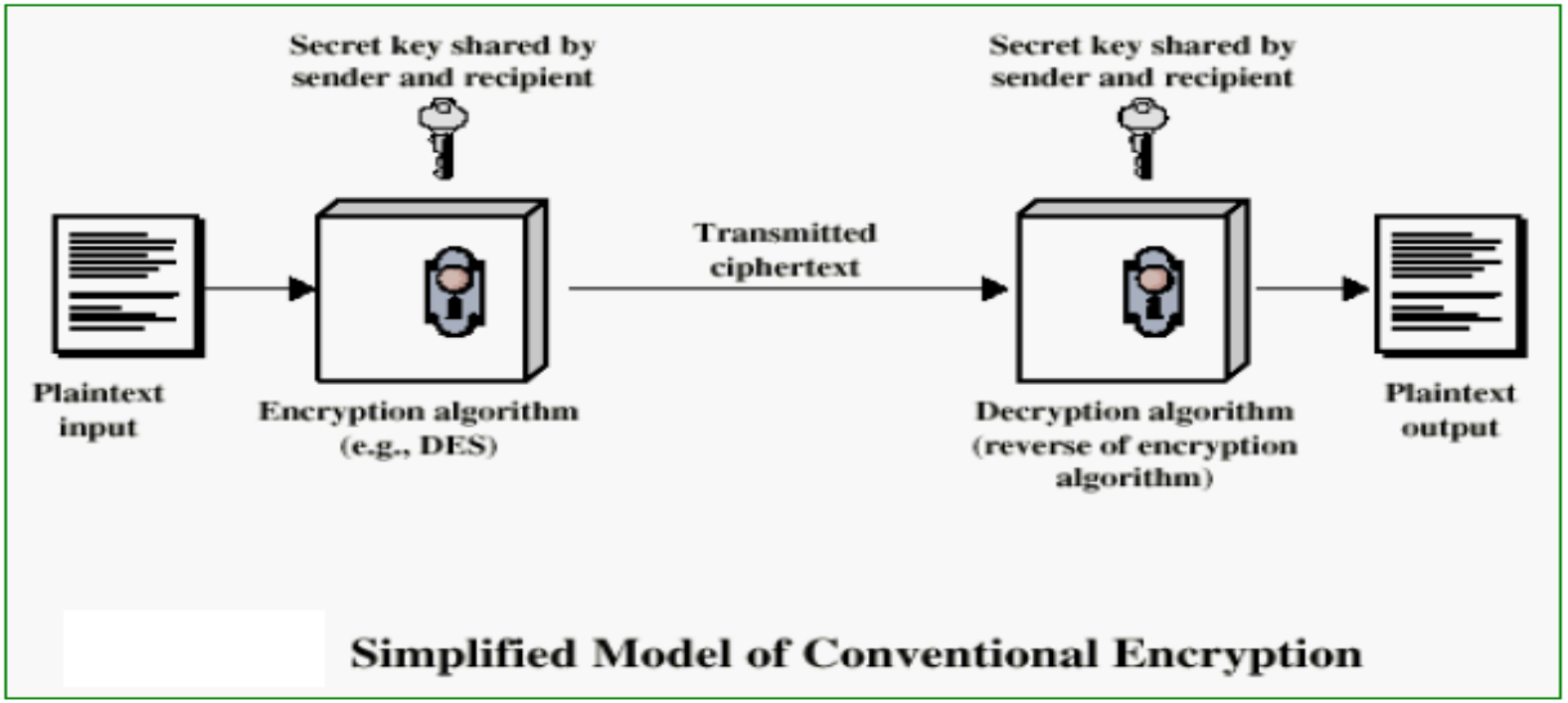
Récepteur: Entité destinée à recevoir l'information dans une transmission à deux parties. Bob est le récepteur.

Adversaire: Entité qui n'est pas l'expéditeur ni le récepteur et qui tente de déjouer la sécurité d'une transmission à deux parties.

Canal: Moyen de transport de l'information d'une entité à une autre.

Canal sécurisé: Canal où l'adversaire n'a pas la possibilité de lire, de modifier ou d'effacer.

- Un schéma d'encrytion possède 5 ingrédients:
  - Texte en clair (Plaintext)
  - Algorithme d'encryption
  - Clé secrète
  - Texte chiffré (Ciphertext)
  - Algorithme de décryption
- La sécurité dépend de la sécurité de la clé et non de celle de l'algorithme.

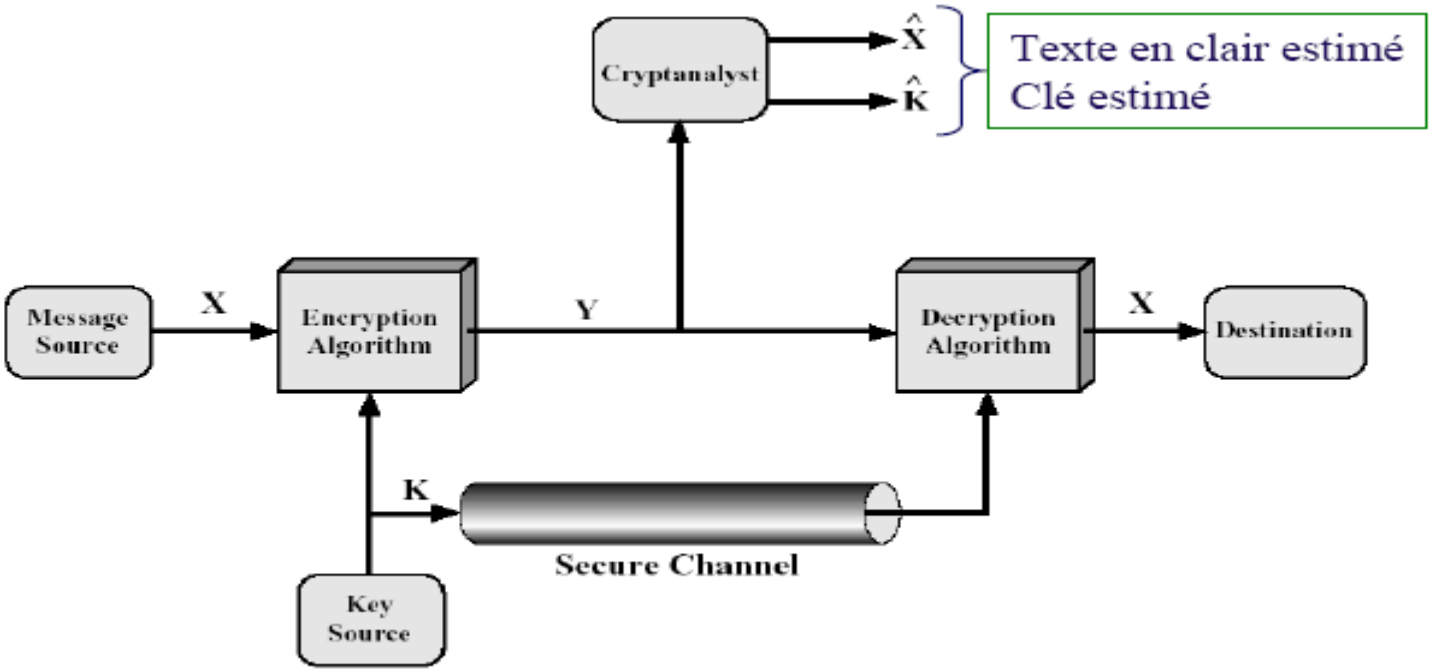


Simplified Model of Conventional Encryption

- Algorithme de chiffrement doit être suffisamment puissant → déchiffrement d'un texte encrypté soit impraticable.
- La sécurité d'un algorithme conventionnel dépend de celle de la clé que de l'algorithme lui même ➔ le secret concerne plutôt la clé

- La source produit du texte en clair $X = [X_1 , X_2 , \ldots, X_M]$, de M lettres
- Une clé est donnée par $K = [K_1 , K_2 , \ldots, K_J]$ est générée
- L'algorithme de chiffrement produira le texte chiffré $Y = [Y_1 , Y_2 , \ldots, Y_N]$
- L'opération de chiffrement et celle de déchiffrement sont représentées par :

$$Y = E_K(X) \quad \Leftrightarrow \quad Y = D_K(X)$$



Cryptanalyse

➪ Objectif : Attaquer un système cryptographique. Un cryptosystème est dit vulnérable s'il est possible de :

- ➜ décrypter des messages sans connaître la clé.
- ➜ encrypter des messages sans connaître la clé.
- ➜ trouver la clé.

➪ Remarques : L'étude de la sécurité des cryptosystèmes suppose l'existance cryptanalystes ayant :

- ➜ suffisamment d'intelligence pour trouver des failles dans les cryptosystèmes lorsqu'elles existent.
- ➜ les ordinateurs les plus puissants pour monter leur attaques.

En d'autres termes, on raisonne toujours par rapport au pire cas.

Classification des attaques

- Attaques : elles peuvent être classifiées selon les informations disponibles aux cryptanalystes.
  - Attaque à texte chiffré : l'analyste dispose de textes chiffrés $c_1, \ldots, c_n$ et cherche à trouver leurs correspondants en clair.
  - Attaque à texte clair : l'analyste dispose de textes en clair $m_1, \ldots, m_n$ et de leurs chiffrements $c_1, \ldots, c_n$ respectifs et essaye de trouver la clé du cryptage ou de décrypter d'autres textes.
  - Attaque à texte clair choisi : l'analyste peut choisir des textes clairs et obtenir leurs textes chiffrés correspondants. En ayant ces connaissances, il essaye de trouver la clé du cryptage ou de décrypter d'autres textes.
  - Etc.

Sécurité d'un cryptosystème

- Évaluation d'un cryptosystème : La sécurité d'un cryptosystème peut se mesurer par le degré de difficulté pour le casser.
  - Inconditionnellement sûr : si un cryptanalyste ne peut pas trouver le texte en clair, quelle que soit les ressources dont il dispose.
  - Algorithmiquement sûr : si le cryptosystème ne peut être cassé avec les ressources disponibles dans un temps raisonnable.

Méthodologie de cryptanalyse

➪ Techniques :

- ➜ Bien comprendre le système cryptographique en question.
- ➜ Dégager ses propriétés.
- ➜ Exploiter ses propriétés pour en déduire ses faiblesses.

Les techniques cryptographiques classiques

- basées sur deux opérations : **substitution** et **transposition**
  - → substitution : remplacer des lettres par d'autres lettres
  - → transposition : les lettres arrangées suivant des ordres différents

les chiffrements peuvent être :
- **monoalphabétique** – seule une substitution/ transposition est appliquée
- **polyalphabétique** - plusieurs substitutions/ transpositions sont utilisées
- Combinaison des deux (**product cipher**)

Chiffrement monoalphabétique

Il s'agit de remplacer chaque caractère du texte en clair par un autre caractère
Soit lettres , nombres ou symboles.

Texte en clair : meet me after the toga party
Texte chiffré : PHHW PH DIWHU WKH WRJD SDUWB

Dans ce cas-ci l'alphabet a été déalée de sorte que le Z est suivi par A
Ce type de chiffrement est connu sous "Ceaser Cipher"

Exemple (Chiffrement de César)

Alphabet en clair : a b c d e f g h I j k l m n o p q r s t u v x y z

Chiffrement : D E F G H I J K L M N O P Q R S T U V X Y Z A B C

Si on assigne un nombre à chaque lettre tq : a = 1, b = 2, …, z = 26

Alors chaque lettre du texte en clair p sera substitué par C, comme suit :

$$C = E(p) = (p+3) \bmod(26)$$

Dans le cas général, si l'aphabet chiffré subit un décalage de k lettre

$$C = E(p) = (p+k) \bmod(26) \quad \text{avec} \quad 1{:}k{:}25$$

L'algorithme de déchiffrement,substitution inverse, est simplement donné par :

$$p = D(C) = (C-k) \bmod(26)$$

Une recherche exhaustive, cryptanalyse avec attaque en force, recouvrera

La clé avec un essai de 25 clés possibles.

Exemple:

Texte en clair : PHHW PH DIWHU WKH WRJD SDUWB

Clé: K = 1 oggv og chvgt vjg vqic rctva

.....

K = 3 meet me after the toga party

.....

K = 25 qiix qi ejxiv xli xske tevxc

➔Trois points importants nous permettent l'usage de l'attaque en force:

- Les algorthmes de chiffrement et de déchiffrement son connus
- Il existe 25 clés possibles
- Le langage du texte en clair est connu et facilement reconnaissable (les textes compressés sont exclus)

➪ Exemple : Le message crypté est $C = JZCBM\ NWZKM$

$K = 0 \Rightarrow D_0(C) = JZCBM\ NWZKM$

$K = 1 \Rightarrow D_1(C) = IYBAL\ MVYJL$

$K = 2 \Rightarrow D_2(C) = HXAZK\ LUXIK$

$K = 3 \Rightarrow D_3(C) = GWZYJ\ KTWHJ$

$K = 4 \Rightarrow D_4(C) = FVYXI\ JSVGI$

$K = 5 \Rightarrow D_5(C) = EUXWH\ IRUFH$

$K = 6 \Rightarrow D_6(C) = DTWVG\ HQTEG$

$K = 7 \Rightarrow D_7(C) = CSVUF\ GPSDF$

$K = 8 \Rightarrow D_8(C) = BRUTE\ FORCE$

Aha ! j'ai trouvé la clé $K = 8$

Recherche exhaustive de la clé

- Limites : Pour que cette technique soit réalisable, il faut que l'espace de clé ait une taille raisonnable.
  - Question : Peut-on appliquer cette technique, par exemple, sur le chiffrement du Vigenere avec un clé de taille 20
  - Réponse : Non, il y a trop de clé à explorer 26^{20}
  - Question : C'est peut être trop pour un humain, mais est ce que c'est trop pour un ordinateur qui peut faire 2 milliard d'opérations par secondes ($2Ghz = 2 * 10^9 o.p.s$) ?

Recherche exhaustive de la clé

- Limites (suite) :
  - Réponse : Oui c'est encore trop pour un ordinateur. En effet :
    - Avec un ordinateur de cette puissance (2Ghz), il faut :

$$\frac{26^{20}}{2*10^9} \approx 996407444760470 4576 \text{ secondes}$$

$$\approx 16606790746007 8409 \text{ minutes}$$

$$\approx 276779845766 7973 \text{ heures}$$

$$\approx 11532493573616 5 \text{ jours}$$

$$\approx 31509545283 1 \text{ années}$$

$$\approx 315 \text{ milliard d'années}$$

Recherche exhaustive de la clé

- Limites (suite) : Supposons qu'on a des capacités infinies (des ordinateurs ultra-puissants et que nous sommes éternel !).
  - Question : La recherche exhaustive nous permet-elle de casser n'importe qu'elle système qui utilise un nombre fini de clés ?
  - Réponse : Pas de tout ! En effet :
    - cette technique repose sur le fait que seule la bonne clé puisse déchiffrer un message crypté en un message qui a un "sens".

      – Exemple : Le message crypté est $C = JZCBM\ NWZKM$

$K = 0 \Rightarrow D_0(C) = JZCBM\ NWZKM$
$K = 1 \Rightarrow D_1(C) = IYBAL\ MVYJL$
$K = 2 \Rightarrow D_2(C) = HXAZK\ LUXIK$
$K = 3 \Rightarrow D_3(C) = GWZYJ\ KTWHJ$
$K = 4 \Rightarrow D_4(C) = FVYXI\ JSVGI$
$K = 5 \Rightarrow D_5(C) = EUXWH\ IRUFH$
$K = 6 \Rightarrow D_6(C) = DTWVG\ HQTEG$
$K = 7 \Rightarrow D_7(C) = CSVUF\ GPSDF$
$K = 8 \Rightarrow D_8(C) = BRUTE\ FORCE$
Aha ! j'ai trouvé la clé $K = 8$

Recherche exhaustive de la clé

Limites (suite) :

- Qu'adviendra t-il si toutes les clés ou une grande partie d'entre elles donnent des textes qui ont un "sens". Laquelle de ces clés est la bonne ?
  - Exemple 1 : Le message crypté avec le chiffrement par décalage est $C = WNAJW$.

$$K = 5 \Rightarrow D_5(C) = river$$
$$K = 22 \Rightarrow D_{10}(C) = arena$$

Analyse de fréquences

➪ Origine : Approche introduite par Abu Youssif Al-Kindi (IXe ciècle)

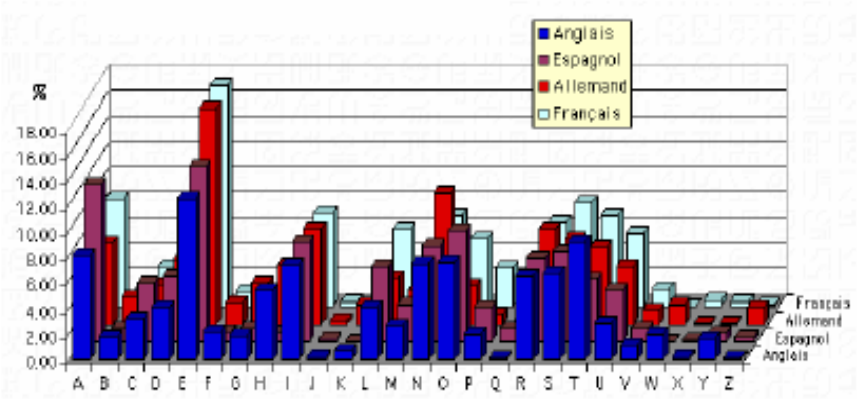
➪ Idée :

- ➜ Établir la fréquence de chaque lettre de l'alphabet. En français la lettre la plus fréquente est 'e' suivie par 'a' puis par 'i', etc.
- ➜ Examiner les fréquences des caractères dans le texte chiffré.
- ➜ Remplacer les caractères les plus fréquents du texte chiffré par les caractères les plus fréquents du langage.
- ➜ Si par exemple la lettre la plus fréquente du texte chiffré est 'j', suivie par 'm', suivie par 'k' alors on fait un premier essai en remplaçant 'j' par 'e', 'm' par 'a' et 'k' par 'i'

Analyse de fréquences

- Idée (suite) : D'une manière plus générale, l'idée est :
  - d'utiliser des statistiques (fréquences de monogramme, fréquence de bigrammes, etc.) sur le système cryptographique.
  - de déduire par la suite des informations sur le système cryptographhques, la clé, etc.

- Fréquences des lettres dans différentes langues :



Exemple

Étant le texte chiffré suivant:

UZQSOVUQHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
VUEPHZHMDZSHZOWSFPPAPPDTSVPQUZWYMXUZUHSX
EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ

1) Le calcul des fréquences et comparaison avec la distribution des lettres anglaises

P=13.33	H=5.83	F=3.33	B=1.67	C=0.00
Z=11.67	D=5.00	W=3.33	G=1.67	K=0.00
S=8.33	E=5.00	Q=2.50	Y=1.67	L=0.00
U=8.33	V=4.17	T=2.50	I=0.83	N=0.00
O=7.50	X=4.17	A=1.67	J=0.83	R=0.00
M=6.67				

Par comparaison, il est probable que: P ⇔ e et Z ⇔ t des suppositions:

Pour les lettres à fréq élevée : {S,U,O,M,H} ⇔ {r,n,i,o,a,s}
Pour les lettres à basse fréq : {A,B,G,Y,I,J} ⇔ {w,v,b,k,x,q,j,z}

2) On peut aussi se baser sur certaines régularités tq mots connus qui se répétent

Si on regarde la séquence ZWSZ, si elle forme un seul mot : th_t ➔ S ⇔ a

UZQSOVUQHXMOPVGPOZPEVSG**ZWSZ**OPFPESXUDBMETSXAIZ
t a e e te a that e e a a
VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
e t ta t hae ee a e th t a
EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ
e e e tat e the t

4 lettres identifiées. On continue le traitement et on about it à remplir l'espace.

it was disclosed yesterday that several informal but
direct contacts have been made with political
representatives of the viet in moscow.

Chiffre de Playfair

- Inventer en 1854 par wheatstone, utilisé en 1ère guerre mondiale
- Le plus connu est le chiffrement multi-lettre → il traite les digrammes = 1 unitée
- À base de l'alphabet et d'un mot clé, une matrice 5X5 est construite (I et J = 1 lettre)

Exemple: Mot clé est MONARCHY

M	O	N	A	R
C	H	Y	B	D
E	F	G	I/J	K
L	P	Q	S	T
U	V	W	X	Z

Séparer les lettres doubles par x (ex de lettre filler)

balloon → ba lx lo on

Lettres même rangée remplacées par celles de droite

ar ⇔ RM

Lettres même colonne remplacées par celles de dessous

mu ⇔ CM

Sinon, chaque digramme est chiffré selon leurs rangée et colonne

hs ⇔ BP et ea ⇔ IM (ou JM)

Chiffre de Hill

- Chiffrement multilettres intéressant développer en 1929
- Substitution simple par des polygrammes → chiffrement en blocs
- L'algorithme remplace m lettres successives du texte en clair par m lettres cryptées
- La substitution se fait à l'aide de m équations linéaires où à chaque lettre est assigné une valeur numérique tq (a=0, b=1, …, z=25)

Exemple: m = 3 $\quad C_1 = k_{11}p_1 + k_{12}p_2 + k_{13}p_3 \bmod 26$

$C_2 = k_{21}p_1 + k_{22}p_2 + k_{23}p_3 \bmod 26 \quad \rightarrow \quad [C] = [K].[P]$

$C_3 = k_{31}p_1 + k_{32}p_2 + k_{33}p_3 \bmod 26 \qquad$ (clé)

Étant donné le texte en clair "paymoremoney" avec $[K] = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 12 \end{pmatrix}$

K(pay) = K(15 0 24) = (375 819 486) mod 26 = (11 13 18) = LNS

Finalement, paymoremoney ⇔ LNSHDLEWMTRW

- Déchiffrement se fait par la matrice inverse K^{-1} tq $K.K^{-1} = I \rightarrow K^{-1} = \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix}$
- Bienqu'il soit inattaquable connaissant seulement le texte chiffré, il est cependant possible de le casser en ayant aussi le texte en clair.

  → à partir de $Y = XK$ on retrouve $K = X^{-1} Y$

Chiffres à substitution polyalphatétique

- Utilisation de différents chiffres monalphabétiques au texte en clair.
- Composé d'un ensmble de règles de substitution monoalph. et d'une clé.
- Chiffre de **Vigenère** est le + connu, basé sur les 26 chiffres de César décalés de 0 à 26

Tableau moderne de Vigenère

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
a	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
b	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
c	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
d	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
e	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
f	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
g	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
h	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
i	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
j	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
k	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
l	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
m	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
n	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
o	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
p	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
r	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
s	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
t	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
u	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
v	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
w	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
x	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Exemple clé: deceptivedeceptivedeceptive

texte en claire : wearediscoveredsaveyourself

texte chiffré : ZIKVTWQNGRZGVTWAVZHCQYGLMGJ

- La puissance de ce chiffre est qu'il assigne à la même lettre plusieurs lettres, donc pas d'information sur la fréquence.
- Le cryptanalyste peut distinguer le chiffre de Playfair de celui de Vigenère, puisque celui de Playfair le texte en clair et le texte chiffré ont les mêmes statistiques sur les lettres
- La cryptanalyse du chiffre de Vigenère dépend de la longueur de la clé. On peut alors évitier la répétition de la clé en utilisant une clé aussi longue que le texte en claire.
- Pour éviter toute vulnérabilité la clé doit être choisie de sorte qu'il n'aye aucune corrélation éventuelle entre la clé et le texte en clair.

Chiffre à transposition

- Un chiffre à transposition est un chiffre dans lequel les caractères du texte en clair demeurent inchangés mais dont les positions respectives sont modifées. de différents
- On écrit le texte horizontalement sur une longueur fixe et on relève le texte chiffré verticalement. Une clé peut être ajoutée pour indiquer l'ordre des colonnes.
- Sur une feuille cadrillée, on utilise l'opération inverse.

Exemple 1 texte en claire : meet me after the toga party

m e m a t r h t g p r y écrit diagonalement

e t e f e t e o a a t

texte chiffré : MEMATRHTGPRYETEFETEOAAT relèvé horizontalement

Exemple 2

Clé	4	3	1	2	5	6	7
texte en clair	a	t	t	a	c	k	p
	o	s	t	p	o	n	e
	d	u	n	t	i	l	t
	w	o	a	m	x	y	z

texte chiffré : TTNAAPTMTSUQAODWCOIXANLYPETZ

- Le cryptanalyste peut reconnaître le chiffre à transposition car il manifeste les mêmes fréquences pour les lettres que celui du texte en clair.

• Pour augmenter la performance du chiffre à transposition et le rendre plus sécure, il suffit d'appliquer plus d'une opération. Le résultat donne des permutations plus complexes

Exemple 3

Clé	4	3	1	2	5	6	7
texte en clair	t	t	n	a	a	p	t
	m	t	s	u	o	a	o
	d	w	c	o	I	x	k
	n	l	y	p	e	t	z

texte chiffré : NSCYAUOPTTWLTMDNAOIEPAXTTOKZ

• Pour visualiser l'avantage de cette double transposition, on affecte à chaque lettre un nombre désignant sa position dans le texte en clair.

Le texte original: 01 02 03 04 05 06 07 08 09 10 11 12 13 14
15 16 17 18 19 20 21 22 23 24 25 26 27 28

1ère transposition : 03 10 17 24 04 11 18 25 02 09 16 23 01 08
15 22 05 12 19 26 06 13 20 27 07 14 21 28

On remarque une certaine régularité dans la structure

2e transposition : 17 09 05 27 24 16 12 07 10 02 22 20 03 25
15 13 04 23 19 14 11 01 26 21 18 08 06 28

Permutation loin d'être régulière et assez difficile à cryptanalyser

Appliquer la méthode César pour chiffrer le message suivant :

- Je suis à Londres dans un des rues les plus misérables de la ville. K=7
- Un enfant a dit je sais des poèmes. K=12

Appliquer la méthode playfair pour chiffrer le message suivant :

- Mot clé : victor hugo
-Texte clair : Sa bouche, pale, s'ouvrait ; la mort noyait son œil farouche, ses bras pendants semblaient demander des appuis.

- Texte clair : un ami qui vous veut du bien
- Mot_clé : PLAYFAIR

Chiffrez le message suivant « Rendez-vous ce soir » avec le chiffrement de Hill en utilisant la matrice

$$\begin{pmatrix} 3 & 2 \\ 1 & 3 \end{pmatrix}$$

- ELECTION avec la clé (ou matrice) de chiffrement

$$\begin{pmatrix} 3 & 5 \\ 1 & 2 \end{pmatrix}$$

- MATHEMATIQUE avec la clé $\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$

Trouver les chiffrements de message LA MAISON BLANCHE avec un chiffrement de Hill avec les matrices :

$$A = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 2 & 3 & 1 \end{bmatrix} \text{ et } B = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 2 & 2 & 3 \end{bmatrix}.$$

Trouver le chiffrement de message LA MAISON BLANCHE avec un chiffrement de Vigenère avec la clé XYZ.

- key: monarchie
- plaintext: au secours nous sommes decouverts

- Texte clair : un ami qui vous veut du bien
- Mot_clé : VIGENERE

Sachant que le message a été chiffré par la méthode de Vigenère, en utilisant le mot-clef VICTOR HUGO, quel est le message en clair obtenu en déchiffrant le cryptogramme suivant:

GMPYO EAUBO DBTXQ LKYAL WINES JKUTG GIVXH VSYRC BQUXH RPNVF
JXTXV LTVRS KIKLW SSYNC IVGMS FUPUM VQVNB IHGKO PJGGW KZOXI