Chapitre II

Cryptographie classique

Plan

Notions de base-1-

- ***Cryptosystèmes*** : Ensemble des méthodes de chiffrement et de déchiffrement assure le service de sécurité.
- ***Cryptographie*** : Art de cacher l'information, de la rendre accessible uniquement à un nombre restreint de personnes➔ confidentialité des données.
- ***Cryptanalyses*** : Art de casser des cryptosystèmes
- ***Chiffrement*** : la conversion des données d'un format lisible à un format codé incompréhensible par l'ennemi .
- ***Déchiffrement*** : une fonction permet de retrouver le texte clair à partir du texte chiffré.

Notions de base-2-

- On désigne par:
  - ***M***: le message clair
  - ***C***: le message chiffré
  - ***E***: l'opération de chiffrement
  - ***D :*** l'opération de déchiffrement

$$E(M)=C$$

$$D©=M$$

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

Notions de base-3-

❑ ***Cryptanalyse:***

- Lorsqu'une méthode de cryptanalyse permet de déchiffrer un message chiffré à l'aide d'un cryptosystème, on dit alors que l'algorithme de chiffrement a été « cassé ».
- On a quatre techniques de cryptanalyse (d'attaque):
  1. Sur un texte chiffré seul : retrouver la clé de déchiffrement à partir d'un ou plusieurs textes chiffrés.
  2. A texte clair connu: retrouver la clé de déchiffrement à partir d'un ou plusieurs textes chiffrés, connaissant le texte en clair correspondant.
  3. A texte clair choisi: L'attaquant possède plusieurs paires (texte clair, texte chiffré). Il peut chiffrer un texte clair choisi.
  4. A texte chiffré choisi: L'attaquant possède plusieurs paires (texte clair, texte chiffré). Il peut décrypter un texte chiffré.

Notions de base-4-

- ***Cryptanalyse (suite):***
  - On a quatre résultats possibles:
    1. Cassage partiel: le pirate connaît quelques informations sur le texte en clair.
    2. Cassage local: le pirate connaît quelques informations sur le texte en clair et le texte chiffré
    3. Cassage global: le pirate calcule la fonction de déchiffrement ***D©*** et peut donc déchiffrer tout message.
    4. Cassage complet: le pirate connaît la clé de cryptage .

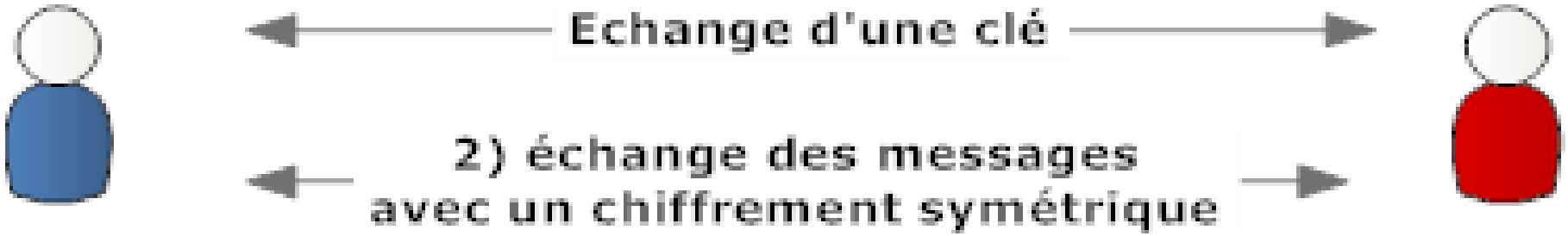
Notions de base-5-

❑ ***Clé symétrique:***

- Les clés sont identiques: $K_E = K_D = K$
- Les clés doit rester secrète entre l'émetteur et le récepteur.
- Les algorithmes qui utilisé le principe du clé symétrique, les plus répondus, sont: DES, AES, 3DES.
- Ces algorithmes sont basés sur des opérations de transposition et de substitution des bits du texte clair en fonction de la clé,
- L'avantage principal de ce mode de chiffrement par clés symétrique est sa rapidité.
- Désavantage: complexité : pour N utilisateurs il faut $\frac{N(N-1)}{2}$ clés

Notions de base-6-

Chiffrement symétrique



Un message chiffré avec la clé est déchiffré avec la même clé.

Le problème : comment transmettre la clé de façon sécurisée ?

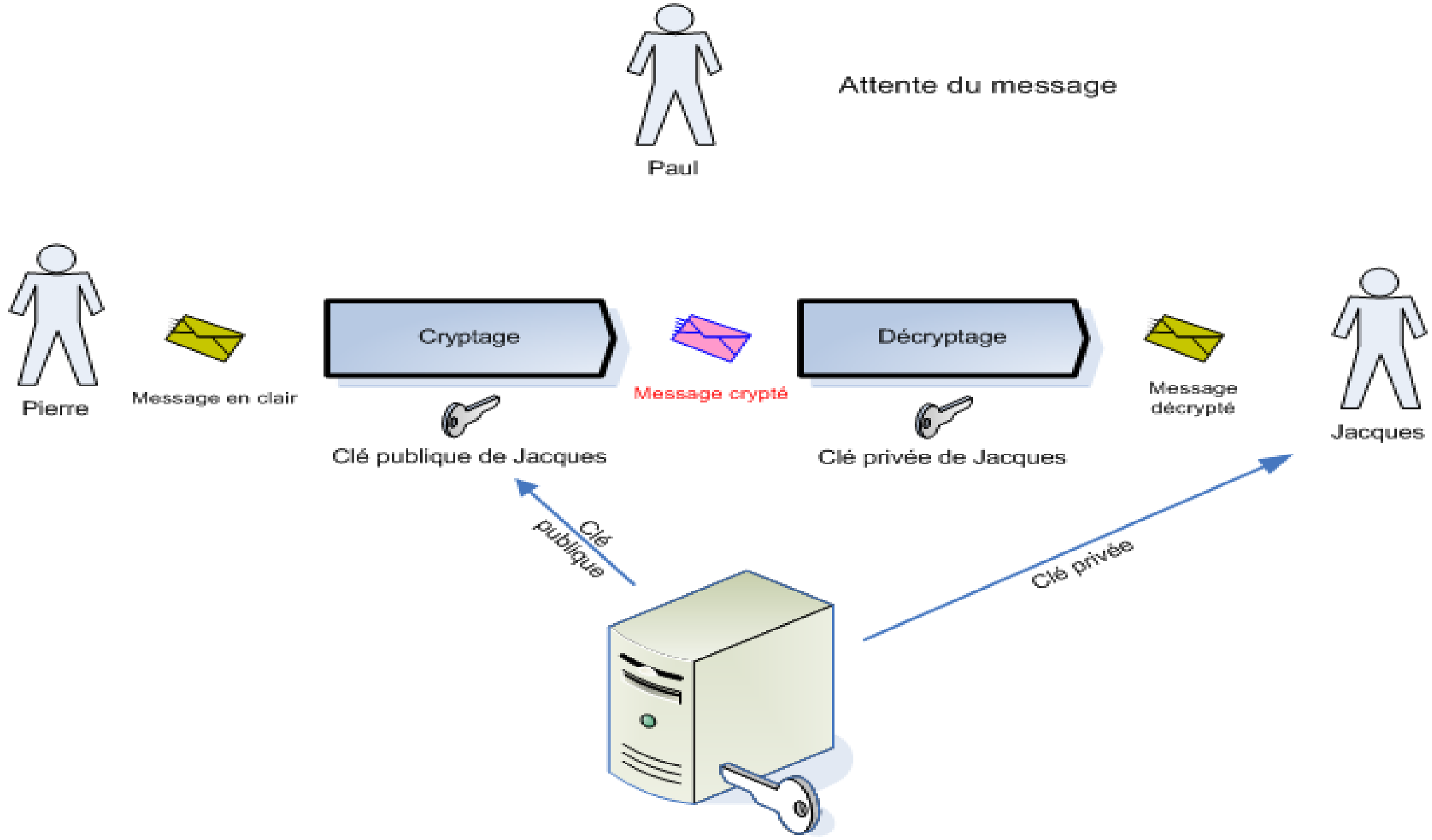
Notions de base-7-

❑ *Clé asymétique:*

- On a une clé publique P_K et une autre clé privée S_k

  ➔**La connaissance de P_K ne permet pas de déduire S_k**

- $D_{S_K}\left(E_{P_K}(M)\right) = M$
- L'algorithme de cryptographie asymétrique le plus connu est le RSA
- Avantage: Très sécurisé: on peut distribuer la clé publique sans risquer que les messages soient déchiffrés
- Désavantage: Le chiffrement par voie asymétrique est environ 1000 fois plus lent que le chiffrement symétrique.


Paul
Attente du message
Pierre
Message en clair
Cryptage
Message crypté
Décryptage
Message décrypté
Jacques
Clé publique de Jacques
Clé privée de Jacques
Clé publique
Clé privée
Serveur de clés publiques sans certificat numérique

Chiffrement par substitution

Définition

- ***Principe :*** substituer un caractère ou un groupe de caractères par un autre dans le texte à chiffrer.
- Plusieurs types de chiffrement par substitution:
  - ***Monoalphabétique***: remplacement de chaque lettre du message par une autre lettre de l'alphabet.
  - ***Polyalphabétique***: c'est une suite de chiffrement momoalphabétique réutilisée périodiquement.
  - ***Polygramme***: basé sur la substitution d'un groupe de caractères dans un message (texte claire) par un autre group de caractères.

Chiffrement par substitution simple

- ***Principe :*** chaque lettre du plaintext est remplacé par un autre de manière unique.
- ***Exemple***:
  - Plaintext: 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
  - Ciphertext: m n b v c x z a s d f g h j k l p o i u y t r e w q
  - Texte claire : bob. How are you.
    Texte crypté: nkn. Akr moc why

Chiffrement de César-1-

❑ ***Principe:*** Décaler les lettres de l'alphabet. Soit ***p*** l'indice de la lettre et ***k***le décalage (alors ***K*** est la clé).

- **Chiffrement:** $\boldsymbol{C = E(p) \equiv p + k[26]}$
- **Déchiffrement:** p= $\boldsymbol{D(C) \equiv C - k[26]}$
- **On a en max 25 clés**

➔ **c'est une chiffrement mono-alphabétique:** Dans un texte en clair, une lettre est toujours substituée par la même lettre.

Chiffrement de César-2-

❑ ***Exemple:***

- Remplacer chaque lettre par celle qui la succède de trois➔k=3.
- L'algorithme est le suivant:
  - **Chiffrement: $C = E(p) = (p + 3)$mod (26)**
  - **Déchiffrement: p= $D(c) = (c - 3)$mod(26)**
  - **Texte claire: bonjour**
  - **Texte chiffré: ERQMRXU**

Cryptanalyse du chiffrement Monoalphabétique-1-

- ***Principe du cryptanalyse:***

  Calculer la fréquence d'apparition de chaque symbole dans le texte crypté et le comparer aux fréquences d'apparition des lettres de l'alphabet dans une langue particulière.

Cryptanalyse du chiffrement Monoalphabétique-3-

- ***Technique de cryptanalyse:***

1. Trouvez les lettres, diagrammes et trigrammes les plus fréquents dans le texte chiffré
2. Suppositions en les associant à ceux les plus fréquents dans un texte claire (dans la langue choisi)

Cryptanalyse du chiffrement Monoalphabétique-3-

- ***En anglais:***
  - **Les lettres** les plus fréquemment utilisé sont : e, t, o, a, n, i, …
  - **Les deux lettres (diagrammes)** les plus fréquemment utilisé sont : th, in, er, re et an.
  - **Les trois lettres (trigrammes))** les plus fréquemment utilisé sont : the, ing, and et ion.

Cryptanalyse du chiffrement Monoalphabétique-4-

Table des fréquences d'apparition des lettres pour un texte français

Lettre	Fréquence %
A	9.42
B	1.02
C	2.64
D	3.39
E	15.87
F	0.95
G	1.04
H	0.77
I	8.41
J	0.89
K	0.00
L	5.34
M	3.24

Lettre	Fréquence %
N	7.15
O	5.14
P	2.86
Q	1.06
R	6.46
S	7.90
T	7.26
U	6.24
V	2.15
W	0.00
X	0.30
Y	0.24
Z	0.32

Cryptanalyse du chiffrement Monoalphabétique-5-

- ***Exemple: Texte chiffré***

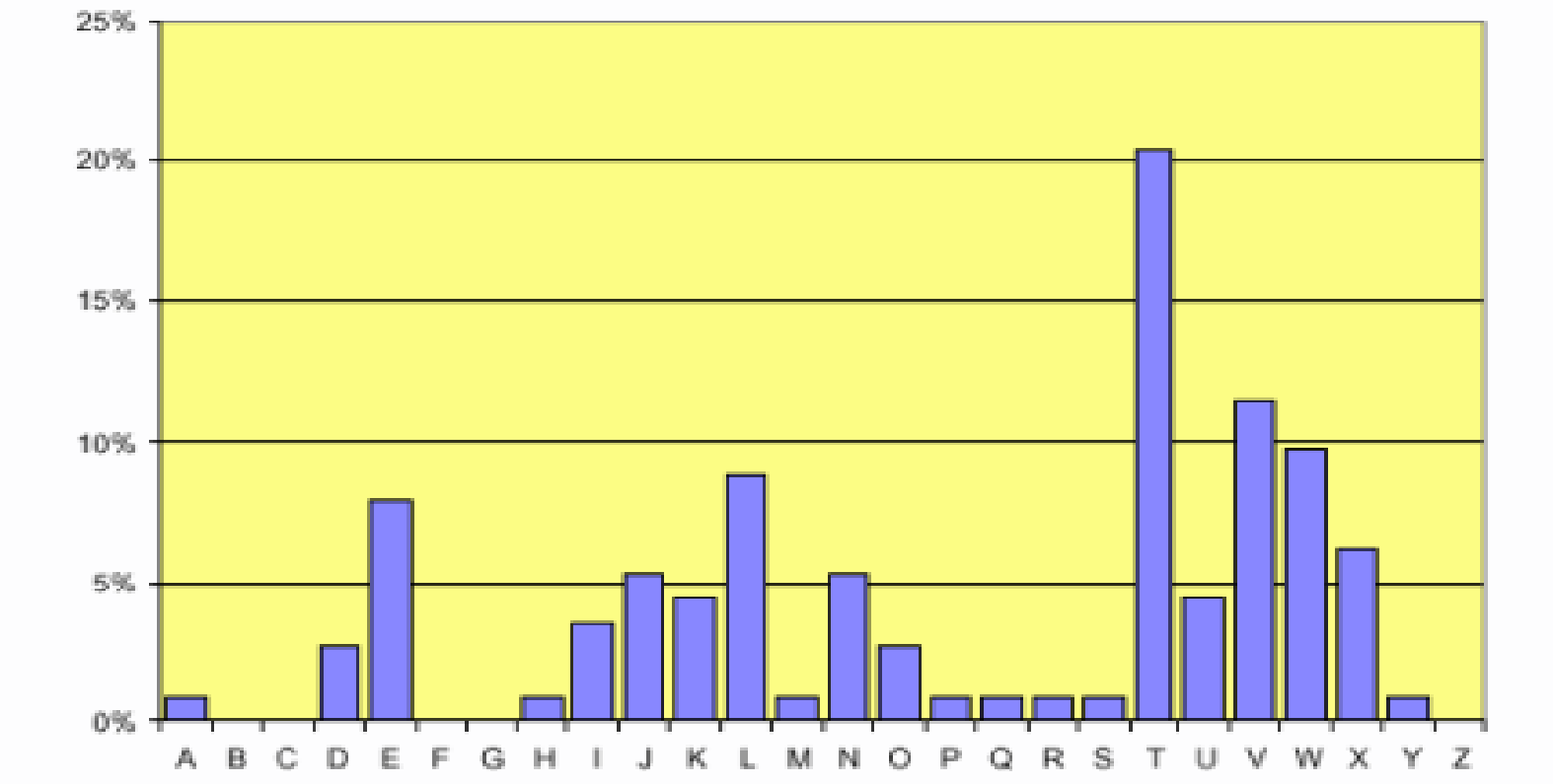
JTVMNKKTVLDEVVTLWTWITKTXUTLWJERUTVTWTHDXATLIUNEWV.

JTVIEVWELOWENLVVNOEDJTVLTPTXYTLWTWUTSNLITTVQXTVXUJX

WEJEWTONKKXLT.

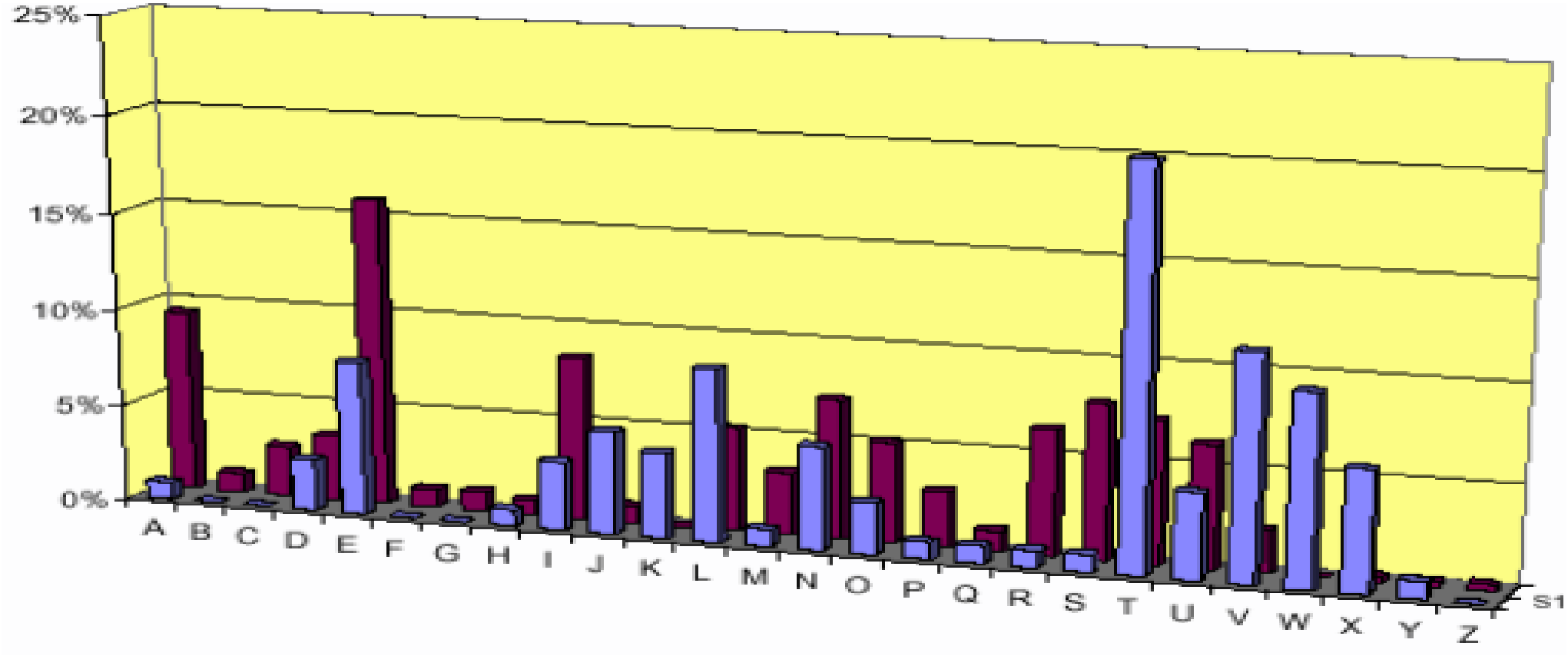
Cryptanalyse du chiffrement Monoalphabétique-6-

Exemple: Analyse des fréquences de caractères du texte chiffré



Cryptanalyse du chiffrement Monoalphabétique-7-

Exemple: Comparaison des fréquences entre texte clair et chiffré



Cryptanalyse du chiffrement Monoalphabétique-8-

- ***Exemple: début du déchiffrement:***

JEVIEVWELOWENLVVNOEDJEVLEPEXYELWEWUESNLI

EEVQXEVXUJXWEJEWEONKKXLE.

Chiffrement affine-1-

- ***C'est une chiffrement par substitution mono-alphabétique***: la lettre d'origine n'est remplacée que par une unique autre lettre
- ***Principe:*** Soit $(\boldsymbol{k_1}, \boldsymbol{k_2}) \in [\mathbf{1}, \mathbf{25}]\boldsymbol{x}[\mathbf{1}, \mathbf{25}]$ les clés et ***x***l'indice de la lettre. Alors $\boldsymbol{k_i}$ est le décalage.
  - **Chiffrement:** $\boldsymbol{C = E(p) \equiv (k_1 x + k_2)[26]}$
  - **Déchiffrement: M**$\equiv \boldsymbol{k_1^{-1}(C - k_2)[26]}$
  - **On a en max 25 clés**

Chiffrement affine-2-

❑ ***Exemple:*** chiffrer le mot CODE grâce au chiffre affine de clef (17,3)

- **Etape I:** On commence par remplacer chaque lettre par son rang dans l'alphabet en commençant au rang 0 (ou rang 1)

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

➢ C O D E → 2; 14; 3 ; 4

Chiffrement affine-3-

- **Etape II:** Appliquer ensuite la fonction affine

  - **2 , 14, 3, 4 → 37,241 ,54, 71**

- **Etape III:** Prendre les restes dans la division par 26

  - **37,241 ,54, 71 → 11, 7, 2,19**

- **Etape IV**: Chiffrement du message

  - 11, 7, 2, 19 → L H C T

Chiffrement affine-4-

- **Etape V:** Retrouvé k_1^{-1} (c'est l'inverse modulaire) qui vérifie
  - $\boldsymbol{k_1 k_1^{-1} \equiv 26 = 1}$
  - $\boldsymbol{k_1^{-1}}$=23
- **Etape VI**: Déchiffrement
  1. Ôte $\boldsymbol{k_2}$ à chaque nombre
  2. Les multiplier par $\boldsymbol{k_1^{-1}}$=23
  3. Chercher les restes dans la division par 26

Chiffrement affine-5-

- L H C T → 11, 7, 2, 19
- 11, 7, 2, 19 → 8, 4, -1, 16
- 8, 4, -1, 16 → 184, 92, -23, 368
- 184, 92, -23, 368 → 2, 14, 3, 4
- 2, 14, 3, 4 → C O D E

Chiffrement de Vigenère-1-

- **C'est une chiffrement *par substitution* polyalphabétique**: basé sur l'utilisation d'une suite de chiffres monoalphabétiques réutilisés périodiquement.

  ➔une lettre peut être chiffrée de façon différente selon sa position dans le texte

- Utilise la même clé pour le chiffrement et le déchiffrement

- ***Principe***: soit un tableau bi-dimensionnel comporter en X et en Y les lettres de l'alphabet, de A à Z.
  - En X, les lettres sont celles du texte en clair,
  - en Y les lettres sont celles de la clé.

Chiffrement de Vigenère-2-

	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

Chiffrement de Vigenère-3-

- ***Chiffrement***:
  1. Faire correspondre toutes les lettres du texte clair avec les lettres de la clé.
  2. Si la clé est inférieure en taille au texte en clair ➔répète la clé autant de fois que nécessaire.
  - Exemple: texte à chiffrer "Chiffre de Vigenere",la clé "clé "

Texte en claire : Chiffre de Vigenere

Clé: cleclec le clecl e cl

3. La i éme lettre chiffré est l'intersection entre la ligne du i éme lettre du texte en claire et la ligne du i ème lettre du clé.

➔Texte chiffré: e s m h q v g hg zkrippvg

c l e c l e c le clecle

Chiffrement de Vigenère-4-

- ***Déchiffrement***: on fait l'inverse mais cette fois on regarde dans <u>la colonne clé</u>

  1. On prend la i éme lettre du clé, et on suit la ligne jusqu'à trouver la i éme lettre du texte chiffré

  2. On remonte pour trouver la i éme lettre du texte en claire

  ➔ Pour notre exemple , la premiere lettre du clé est « C », on prend la lettre c et on suit la ligne jusqu'à trouver la lettre du texte chiffré, E ici.

Chiffrement de Vernam-1-

- Chiffrement de Vernam ou aussi appelé Chiffrement à masque jetable (One Time Pad) est une chiffrement polyalphabétique.
- Principe: on choisit un masque (une suite de bits) aléatoire (la clé), on convertit le texte en clair en une chaîne de bits (suivant le **code ASCII** par exemple) puis on effectue un OU exclusif (XOR) entre ces deux chaînes de bits.
  - **Chiffrement: C = M ⊕ Km**
  - Déchiffrement: M = C ⊕ Km

Chiffrement de Vernam-2-

- ❑ Chiffrement parfait
  - La clé est aussi longue que le message à chiffrer
  - La clé est nouvelle pour chaque nouveau message
- ❑ Confusion totale
  - Chiffrement complètement aléatoire
- ❑Diffusion totale
  - La clé n'est jamais réutilisée : résultat différent à chaque fois.

Chiffrement de Vernam-3-

- Exemple:
  - M=SALUT
  - ➔Conversion en binaire
    - ➔M=**01010011 01000001 01001100 01010101 01010100**

XOR

  - Clé générée aléatoirement
    - ➔**K=01110111 01110111 00100100 00011111 00011010**
    - ➔**C=00100100 00110110 01101000 01001010 01001110**
  - ➔ **Conversion en caractère**
    - ➔C= (M XOR k)= $6jJM

Chiffrement par transposition-1-

- ***Chiffrement par transposition:*** c'est une réarrangement des éléments du texte clair.

- ***Exemple: technique de Rail fence***
  - Le texte clair est réécrit comme une séquence de lignes, puis réordonnée comme une séquence des colonnes

Chiffrement par transposition-2-

- ***Exemple:***

Key: 4 3 1 2 5 6 7
Texte claire: a t t a c k p
o s t p o n e
d u n t i l t

Texte chiffré: TTN APT TSU AOD COI KNL PET