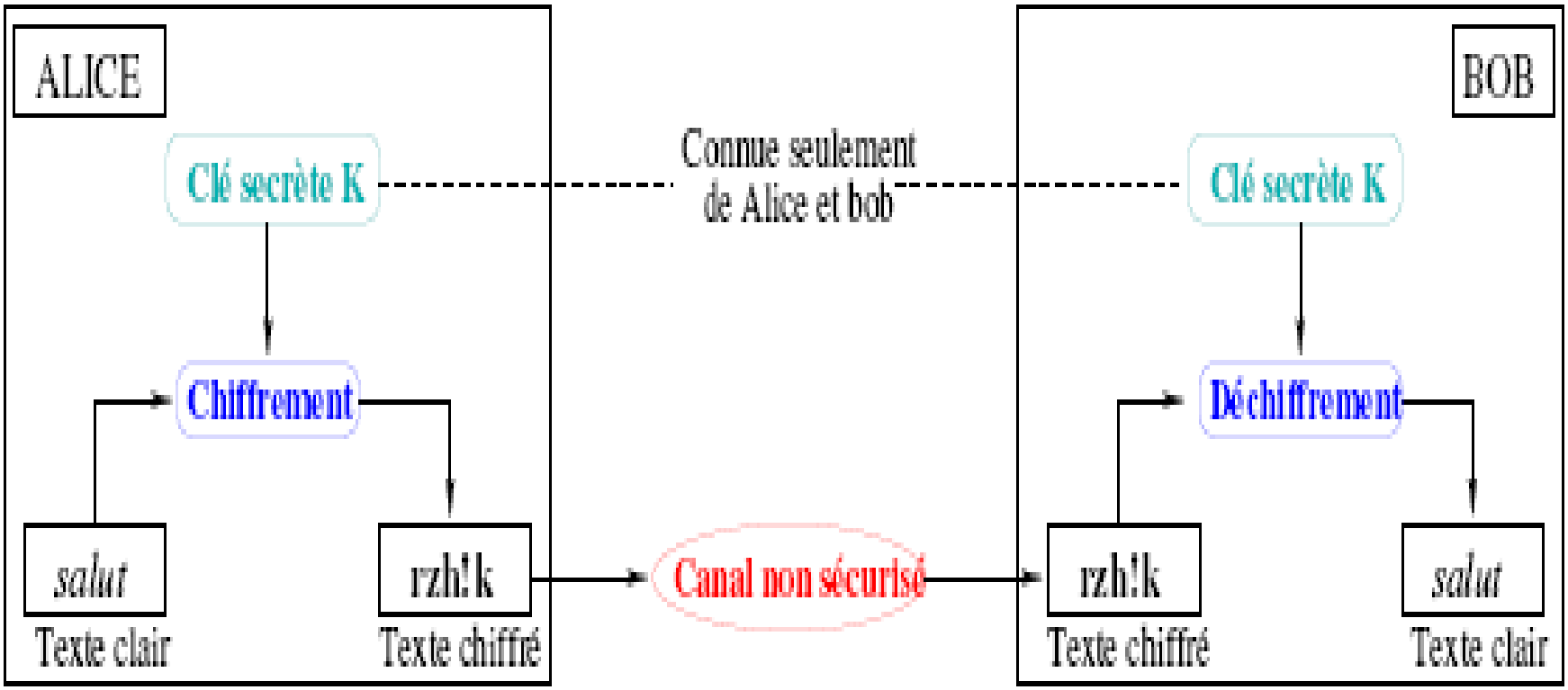
La cryptographie à clé secrète

Partie1 : Cryptographie Classique

Prof: Mme F.Omary

2020-2021

Principe



$K_e = K_d = K$ (clé privée convenue secrètement par Alice et Bob)

Principe (2)

- En pratique: grande efficacité en terme de temps de calcul
- Inconvénient : la clé K doit rester secrète

- Analogie : coffre-fort !
- Historiquement le premier type de chiffrement utilisé.
- Fournit le seul chiffrement théoriquement indéchiffrable
  - Chiffrement de Vernam (one time pad or passeword)
  - Démonstration du mathématicien Claude Shannon 1949

Principe (3)

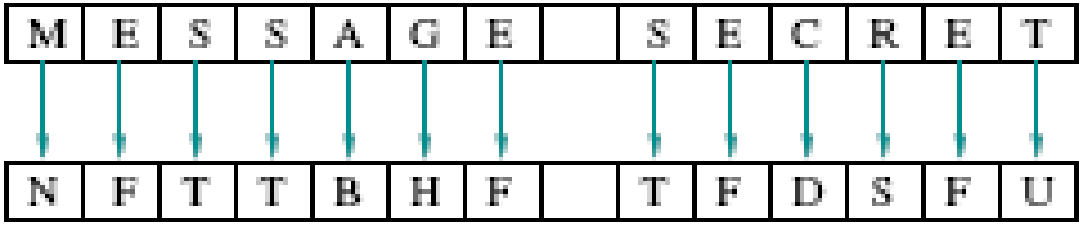
- **Cryptographie symétrique** (cryptographie conventionnelle ou à clé secrète)

  les clefs de chiffrement et de déchiffrement sont identiques: c'est la clef secrète
  - chiffrement en continu ou par flux ou par flot.
  - Chiffrement par bloc
- **Cryptographie asymétrique** (ou à clef publique)

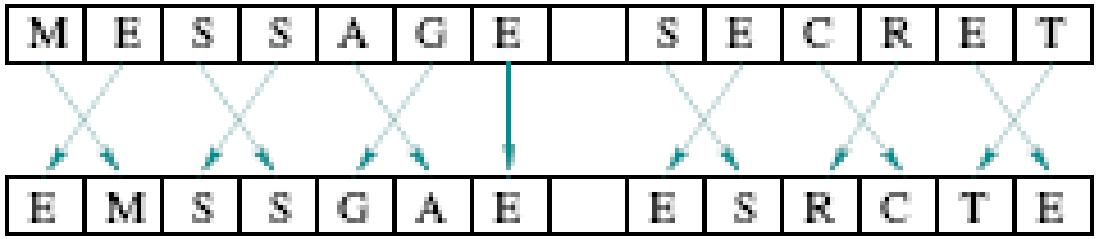
  les clefs de chiffrement et de déchiffrement sont distinctes et ne peuvent se déduire l'une de l'autre

Chiffrement symétrique

- A la base des chiffrements à clé secrète:
  - Substitution : remplacer chaque élément par un autre



  - Transposition : (ou permutation):changer l'ordre des éléments



Opérations utilisées

- Arithmétique modulaire dans Z_n a, b, n $\in$ IN avec n ≥ 2

  $a \equiv b \bmod n \iff$ n divise a-b

  En pratique : b = reste de la division euclidienne de a par n

  $5 \equiv 1 \bmod 4$ et $-3 \equiv 125 \bmod 128$

- Notions ± associées: Primalité, Euclide, Th. Des restes chinois, Gauss, Euler…
- Opération XOR (ou exclusif $\oplus$)
  - Opération bijective (involutive)
  - Correspond à une addition bit à bit modulo 2

$\oplus$	0	1
0	0	1
1	1	0

Les procédés classiques

- Initialement la technique mise en œuvre était secrète
  - 400 av JC: esclave envoyé à Aristogoras par Histaius
  - Avant JC: premières transpositions mono alphabétiques
    - Chiffrement de type anagramme: mélange les lettres de M
  - Avant J: premières substitutions
    - Chiffrement par changement d'alphabet
  - 150 avant JC : carré de Polybe

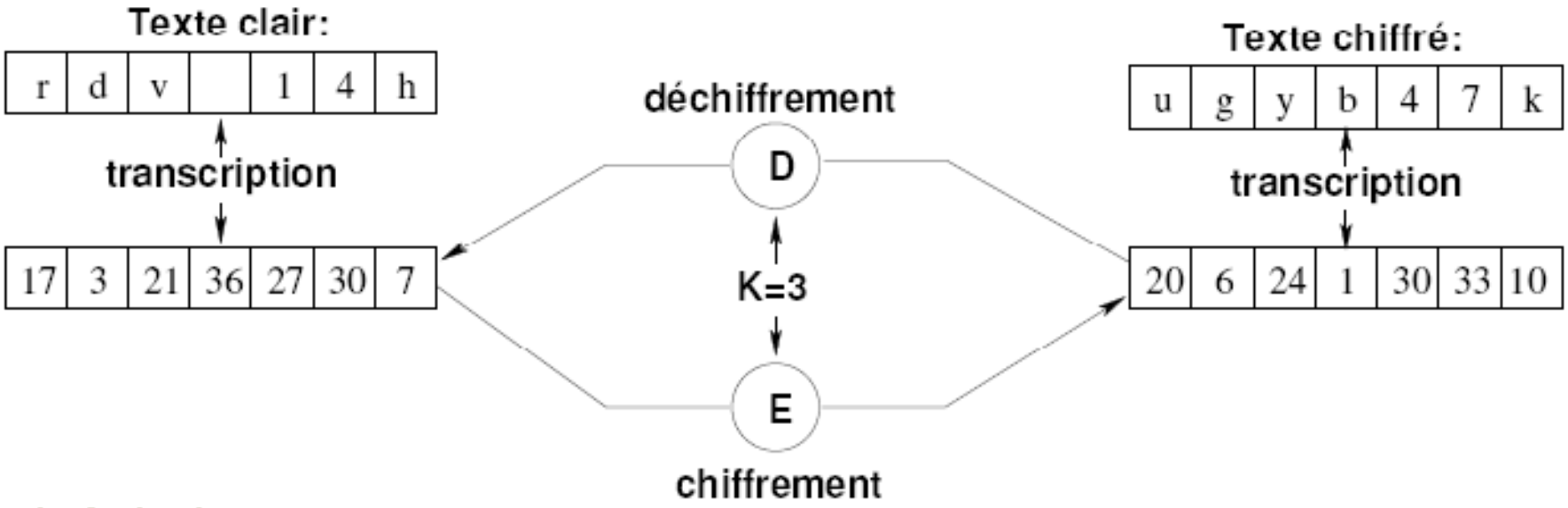
(25 lettres pas de w ou i et j regroupés)

	1	2	3	4	5
1	a	b	c	d	e
2	f	g	h	i	j
3	k	l	m	n	o
4	p	q	r	s	t
5	u	v	x	y	z

Chiffrement de César

- Chiffrement par décalage avec k = 3.

$E_k(M) = M+K \mod n$ $D_k(C) = C-K \mod n$

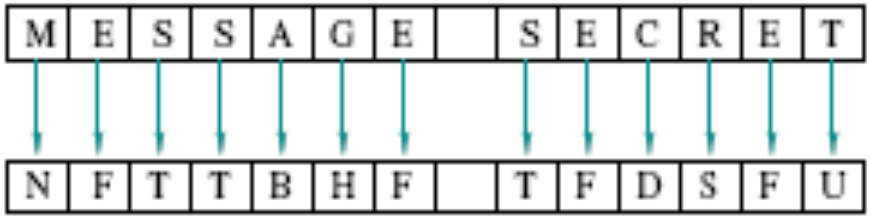


Chiffrement de César (2)

- Seulement n façons différentes de chiffrer un message
  - Code très peu sûr (recherche exhaustive facile)
  - Avantage de la simplicité
    - Employé en armé
    - Réemployé sur les forums de News: (k=13)
- Généralisation: chiffrement affine
  - $E_{(a,b)}(M) = a*M+b \mod n$ pour $a \in Z_n$ et non nul
  - Avec pgcd (a,n)=1 (condition nécessaire et suffisante)

Cryptanalyse des substitutions

- Substitutions mono-alphabétiques: dans une substitution mono-alphabétique on remplace chaque lettre par une lettre différente



Cryptanalyse des substitutions (2)

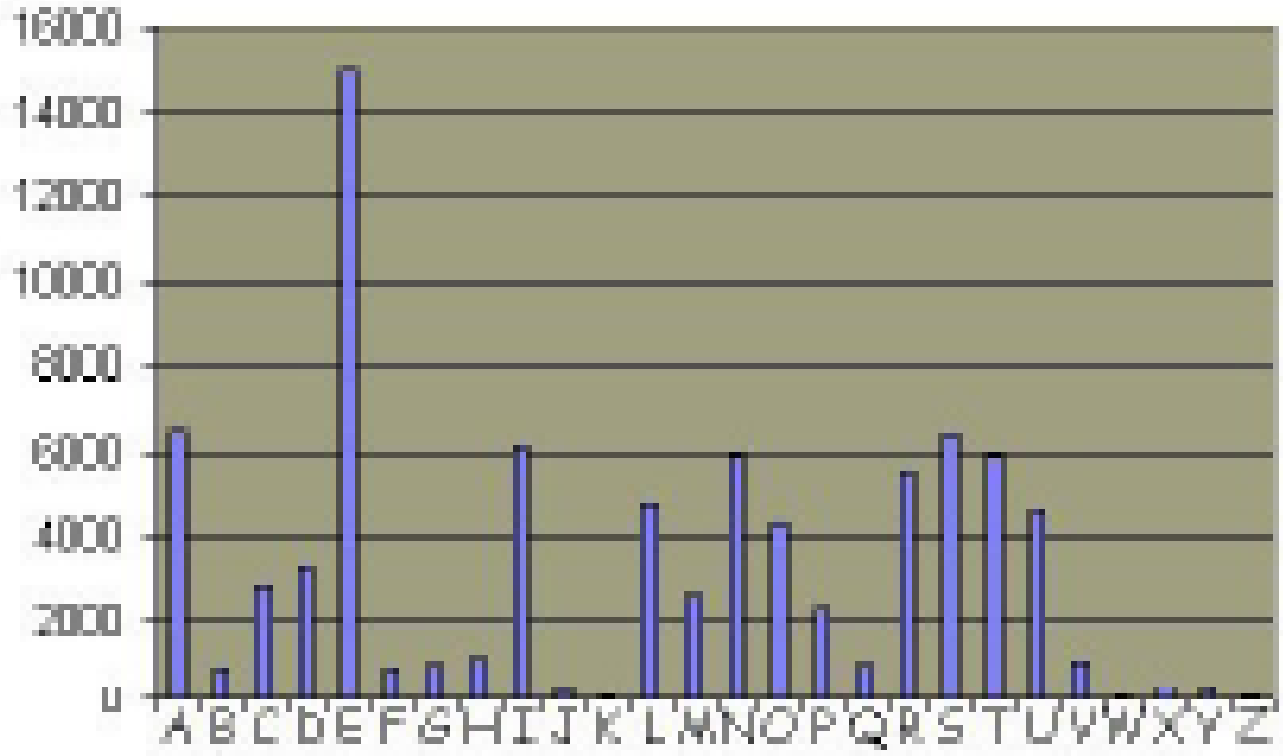
- Nombre de possibilités (alphabet de 26 lettres)
- chiffrement de ‘A’: 26 possibilités
- chiffrement de ‘B’: 25 possibilités

… ⟶ $26! \simeq 4*10^{26}$ possibilités

Mais la fréquence d’apparition des symboles n’ est pas cachée

En français, la lettre’e’ apparaît le plus souvent …

Cryptanalyse des substitutions(3)



Cryptanalyse des substitutions(4)

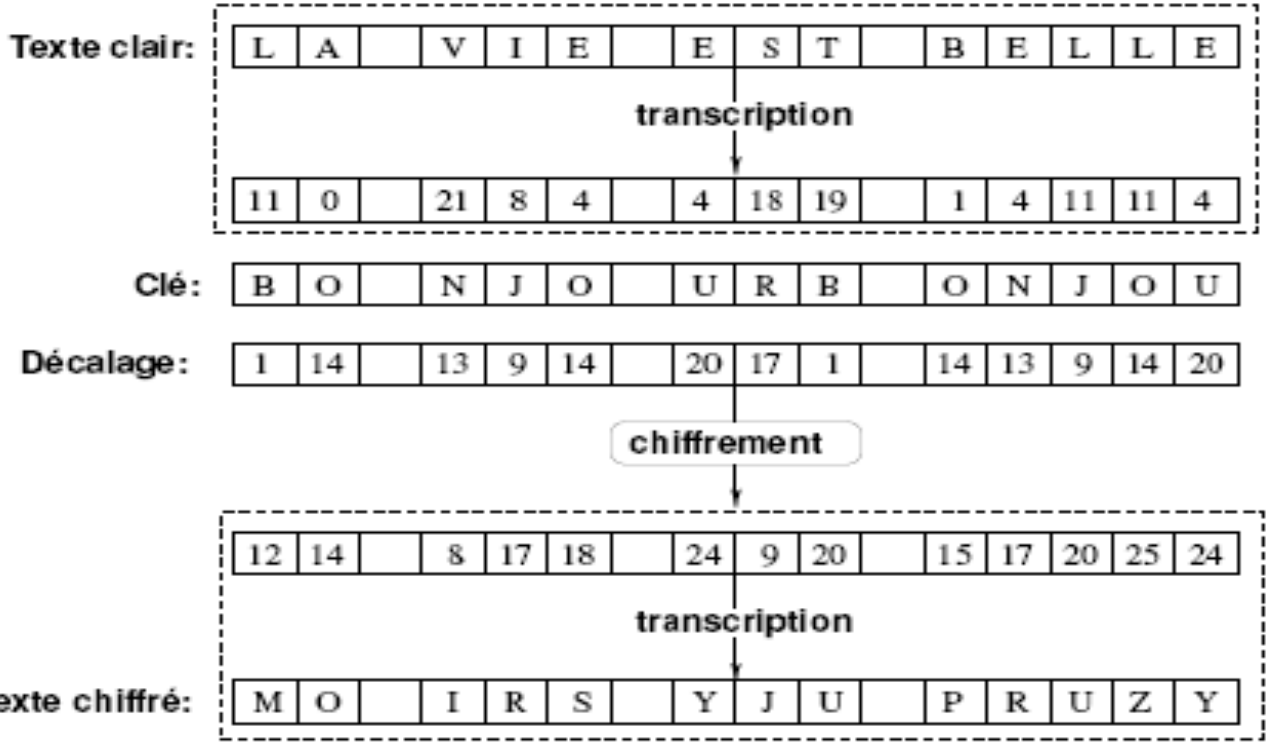
- Exemple: cryptanalyse du texte suivant (enTD)

HQYRBHU GX UHQIRUW DYHF GHV DUPHV

- Cryptanalyse proposée par Al Kindi (TD)

Substitution polyalphabétique (1)

- Méthode utilisée par Vigenère (1586)
- La clef (***mot-clef***) de m caractères peut transformer un caractère du message clair en m caractères #



Substitution polyalphabétique (2)

- Procédé de Vigenère résistera jusqu'au milieu du XIX s.
  - Cryptanalyse de Babbage (1854) et Kasiski(1863)

    Principe:- Deux segments identiques du texte clair décalés de ***p*** positions sont chiffrés de la même manière dès que ***p*** est multiple de m.

    -Inversement, si deux segments sont identiques dans le texte chiffré et de longueur au moins trois, il y'a forte chance qu'ils proviennent de segments identiques du texte clair.
  - But : Déterminer la longueur du mot-clef, notée m.

Substitution polyalphabétique(3)

- Vérification de la valeur de m par ***l'indice de coïncidence.*** Notion définie par Wolfe Freidman en 1920.

- Se ramener à la cryptanalyse de substitution simple.

Exemple: En TD

Notion de sécurité inconditionnelle

- Définition (sécurité inconditionnelle)

La connaissance du message chiffré n'apporte aucune information sur le message clair.

- Seule attaque possible: recherche exhaustive de clé secrète
- La clé secrète doit être au moins aussi longue que le texte clair.

Existe-t-il un système cryptographique inconditionnellement sûr?

Système de Vernam (One time pad)

- Relation fondamentale:

$$\forall M, K \,/\, |M| = |K|,\ (M \oplus K) \oplus K = M$$

- Fonctions de chiffrement/déchiffrement

$$\begin{cases} E_K(M) = M \oplus K \\ D_K(C) = C \oplus K \end{cases}$$

- Vigenère avec Longueur mot-clef=longueur message

Système de Vernam (2)

- Pour un message M de n bits, clef K de n bits.

M = 1000011

K = 1101000

C=M $\oplus$ K = 0101011

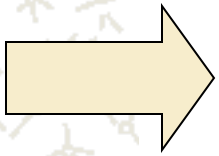
- Si K est totalement aléatoire et n'est utilisée une seule fois

Alors Oscar n'obtient aucune information sur M à partir de C

Systèmes cryptographiques pratiquement sûr

- Vernam : seul système prouvé inconditionnellement sûr
  - Mais problème du caractère aléatoire et du stockage de K
  - Tous les autres systèmes sont théoriquement cassables
- Définition (chiffrement pratiquement sûr)

Un message chiffré ne permet de retrouver ni la clé secrète ni le message clair en un temps humainement raisonnable.



permet d'utiliser des clés plus petites (56, 128 bits…)