# Alice et Bob : une introduction à la cryptographie

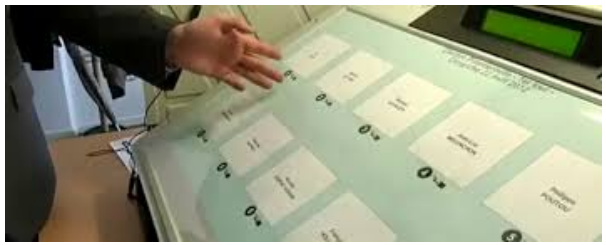
## 2017-2018

IREM de Limoges

Faculté des Sciences & Techniques

# Points communs ?



# Plan

# Plan

# CRYPTOLOGIE

- Cryptographie (étude des méthodes de transmission de données confidentielles, signature numérique, intégrité des données, authentification).

# CRYPTOLOGIE

- Cryptographie (étude des méthodes de transmission de données confidentielles, signature numérique, intégrité des données, authentification).
- Cryptanalyse (étude des procédés cryptographiques afin de trouver des faiblesses, retrouver l'information, détourner, etc. )

# Éthymologie

Crypto graphie
($\kappa\rho\upsilon\pi\tau\omega\rho$ ) Cruptos : caché, dissimulé
( $\gamma\rho\alpha\phi\varepsilon\iota\nu$ ) Graphein : écrire

# Principes généraux

# Principes généraux

**Confidentialité**
Transmettre des données de telle sorte que seul le destinataire autorisé puisse les lire.

# Principes généraux

**Confidentialité**
Transmettre des données de telle sorte que seul le destinataire autorisé puisse les lire.
**Authentification**
Permettre d'identifier des personnes ou des entités et de certifier leur identité.

# Principes généraux

**Confidentialité**
Transmettre des données de telle sorte que seul le destinataire autorisé puisse les lire.
**Authentification**
Permettre d'identifier des personnes ou des entités et de certifier leur identité.
**Intégrité**
S'assurer que les données reçues n'ont pas été modifiées durant la transmission.

# Principes généraux

**Confidentialité**
Transmettre des données de telle sorte que seul le destinataire autorisé puisse les lire.
**Authentification**
Permettre d'identifier des personnes ou des entités et de certifier leur identité.
**Intégrité**
S'assurer que les données reçues n'ont pas été modifiées durant la transmission.
**Non répudiation**
Enregistrer un acte ou un engagement d'une personne ou d'une entité de telle sorte que celle-ci ne puisse pas nier avoir accompli cet acte ou pris cet engagement.

# Plan

# Terminologie

- Les messages que l'on désire envoyer sont écrits dans une langue qui a un **alphabet**.

# Terminologie

- Les messages que l'on désire envoyer sont écrits dans une langue qui a un **alphabet**.
- Un **message clair** est une suite (sensée) de caractères dans l'alphabet donné.

# Terminologie

- Les messages que l'on désire envoyer sont écrits dans une langue qui a un **alphabet**.
- Un **message clair** est une suite (sensée) de caractères dans l'alphabet donné.
- Le message clair est **chiffré** en un **message chiffré** à l'aide d'une **clé de chiffrement**.

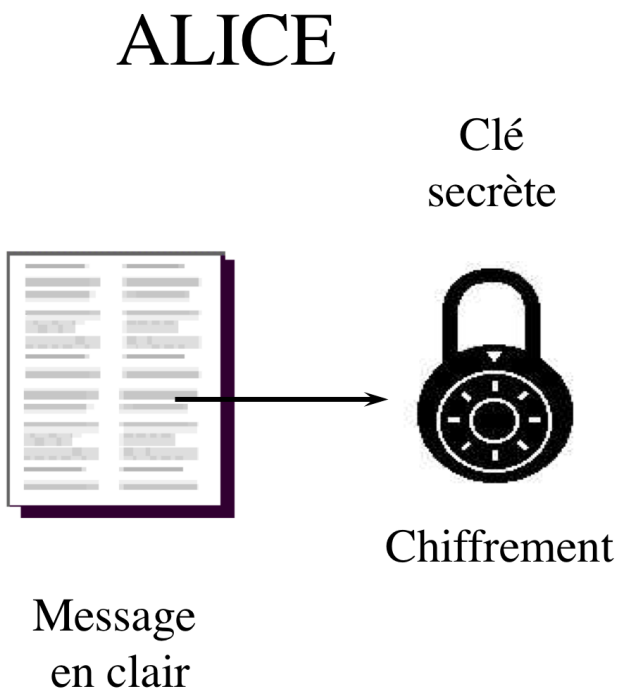
# Terminologie

- Les messages que l'on désire envoyer sont écrits dans une langue qui a un **alphabet**.
- Un **message clair** est une suite (sensée) de caractères dans l'alphabet donné.
- Le message clair est **chiffré** en un **message chiffré** à l'aide d'une **clé de chiffrement**.
- **Le destinataire** du message **déchiffre** le message chiffré à l'aide d'une **clé de déchiffrement**.

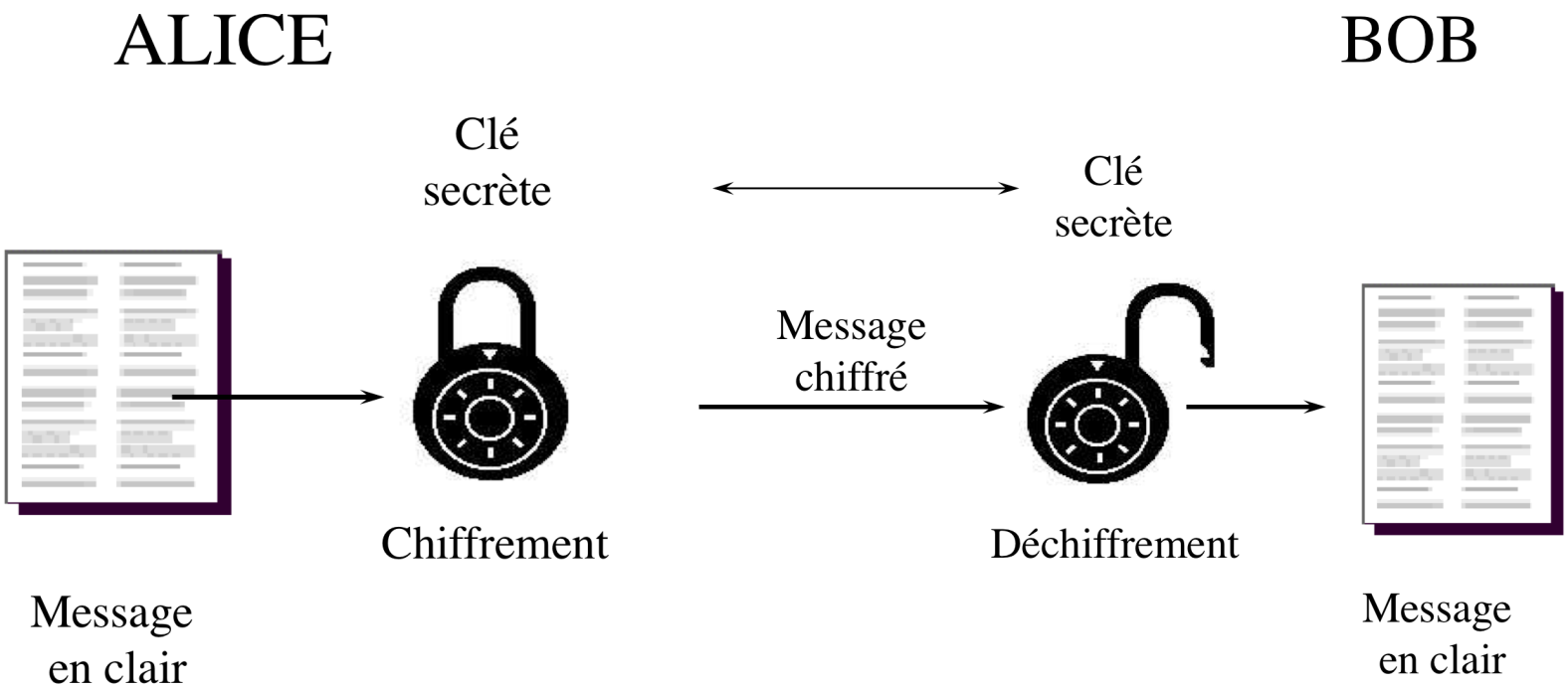
# Terminologie

- Les messages que l'on désire envoyer sont écrits dans une langue qui a un **alphabet**.
- Un **message clair** est une suite (sensée) de caractères dans l'alphabet donné.
- Le message clair est **chiffré** en un **message chiffré** à l'aide d'une **clé de chiffrement**.
- **Le destinataire** du message **déchiffre** le message chiffré à l'aide d'une **clé de déchiffrement**.
- **L'espion décrypte** le message chiffré.

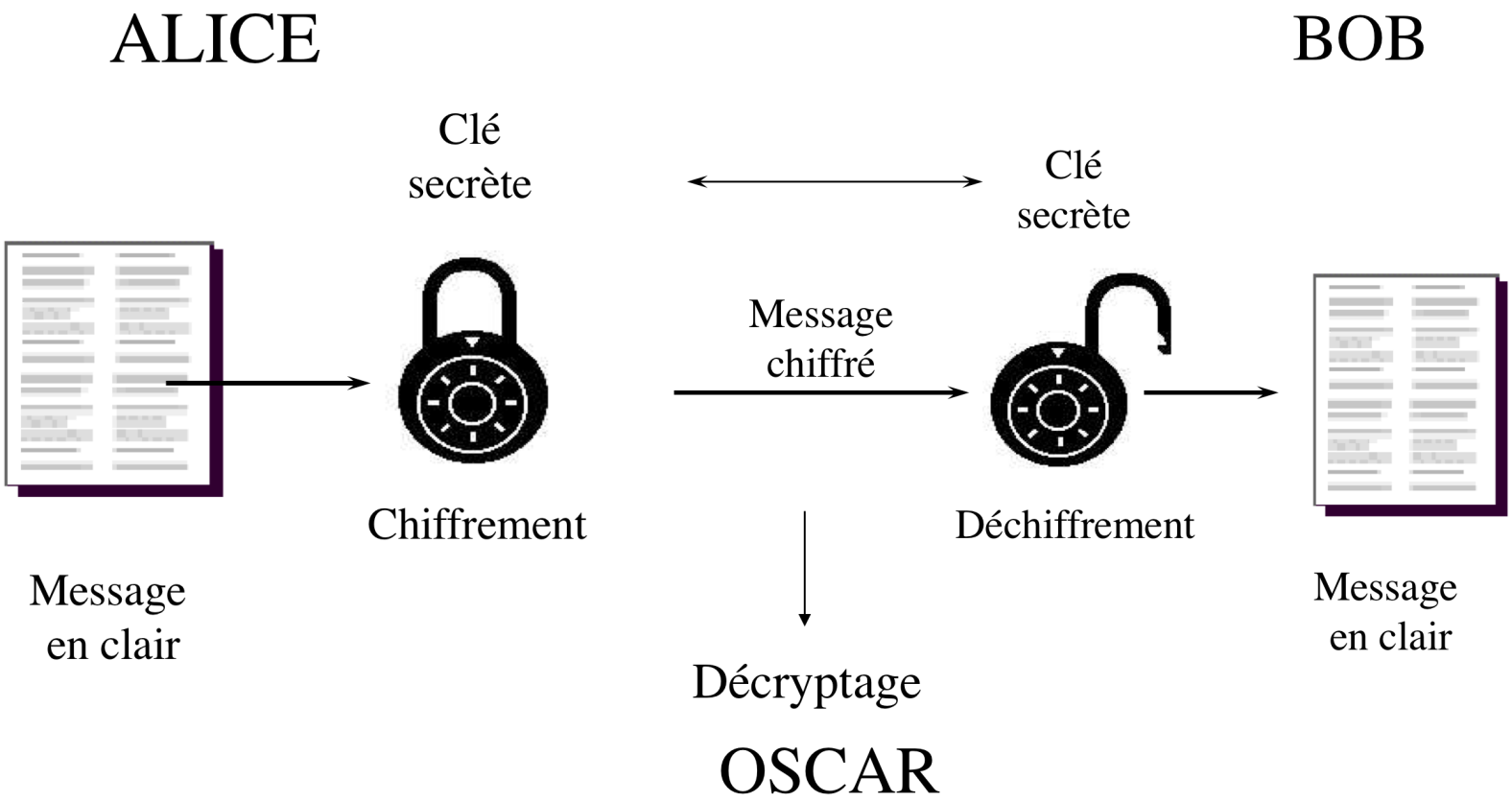
# Terminologie



# Terminologie



# Terminologie



# Plan

# César

# César

# Chiffrement de César

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

**BIENVENUE** $\Rightarrow$

Clé de chiffrement ? de déchiffrement ?

# Chiffrement de César

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

**BIENVENUE** $\Rightarrow$ E

Clé de chiffrement ? de déchiffrement ?

# Chiffrement de César

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

**BIENVENUE** $\Rightarrow$ E L

Clé de chiffrement ? de déchiffrement ?

# Chiffrement de César

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

**BIENVENUE** $\Rightarrow$ E L H

Clé de chiffrement ? de déchiffrement ?

# Chiffrement de César

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

**BIENVENUE** $\Rightarrow$ E L H Q

Clé de chiffrement ? de déchiffrement ?

# Chiffrement de César

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

**BIENVENUE** $\Rightarrow$ E L H Q Y

Clé de chiffrement ? de déchiffrement ?

# Chiffrement de César

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

**BIENVENUE** $\Rightarrow$ E L H Q Y H

Clé de chiffrement ? de déchiffrement ?

# Chiffrement de César

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

**BIENVENUE** $\Rightarrow$ E L H Q Y H Q X

Clé de chiffrement ? de déchiffrement ?

# Chiffrement de César

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

**BIENVENUE** $\Rightarrow$ E L H Q Y H Q X

Clé de chiffrement ? de déchiffrement ?

# Chiffrement de César

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

**BIENVENUE** $\Rightarrow$ E L H Q Y H Q X H

Clé de chiffrement ? de déchiffrement ?

# Codage des lettres

| Lettre | A | B | C | D | E | F | G | H | I | J | K | L | M | N |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| codage | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 10 | 11 | 12 | 13 | 14 |
| Lettre | O | P | Q | R | S | T | U | V | W | X | Y | Z | | |
| codage | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 00 | |

Exemple Rendez vous demain
18 05 04 05 26 00 22 15 21 19 00 04 05 13 01 09 14

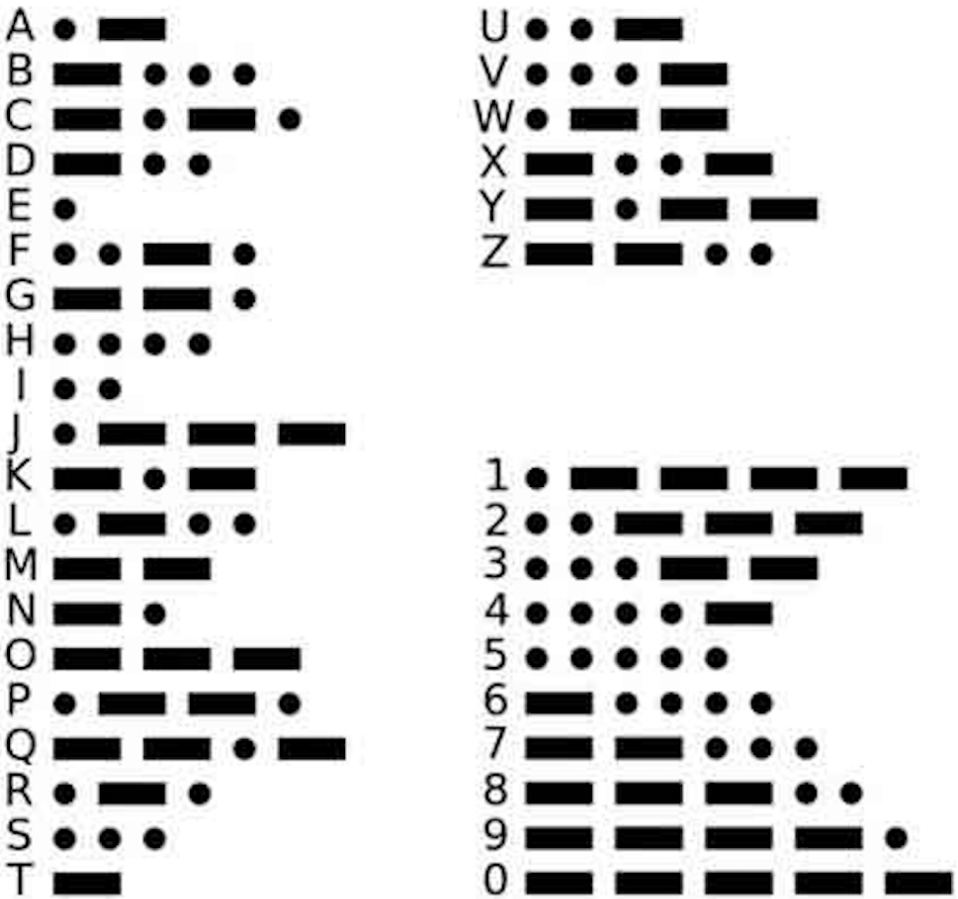
# Chiffrement avec décalage ( +5 modulo 27)

| Lettre | A | B | C | D | E | F | G | H | I | J | K | L | M | N |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| codage | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 10 | 11 | 12 | 13 | 14 |
| chiffr. | 06 | 07 | 08 | 09 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 |
| Lettre | O | P | Q | R | S | T | U | V | W | X | Y | Z | | |
| codage | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 00 | |
| chiffr. | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 00 | 01 | 02 | 03 | 04 | 05 | 06 |

Clé de déchiffrement : $-5$ mod 27

# Plan

# Morse : International Morse Code




The length of a dot is one unit.
A dash is three units.
The space between parts of the same letter is one unit.
The space between letters is three units.
The space between words is seven units.

# Morse : International Morse Code

# Plan

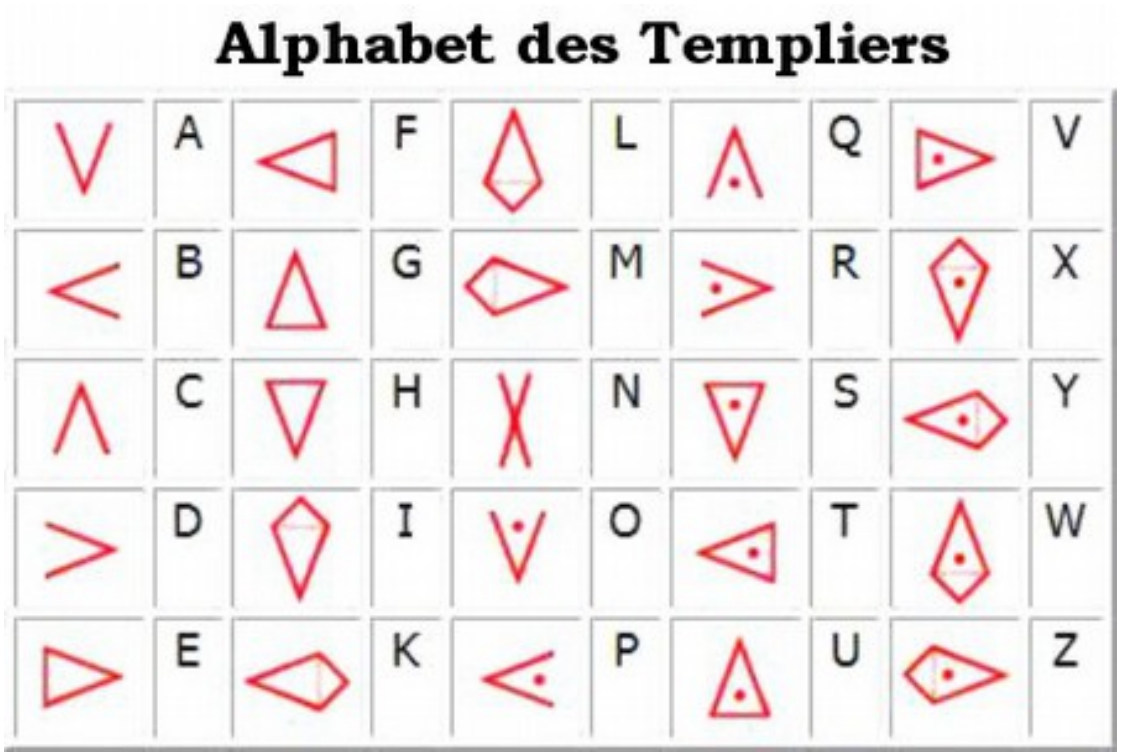
# Les templiers

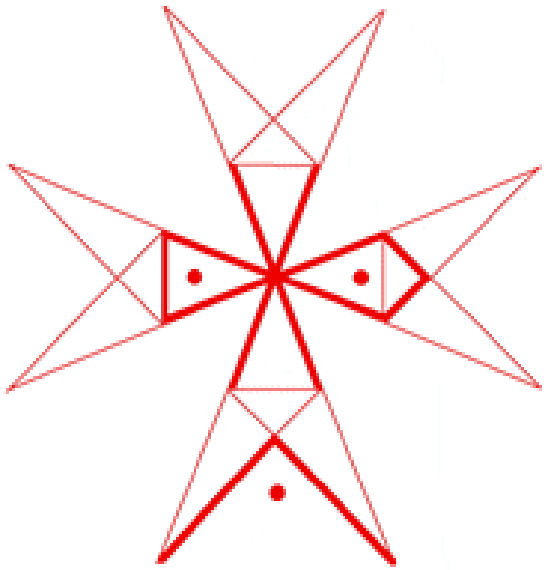
Les templiers, une substitution simple

Croix de Malte

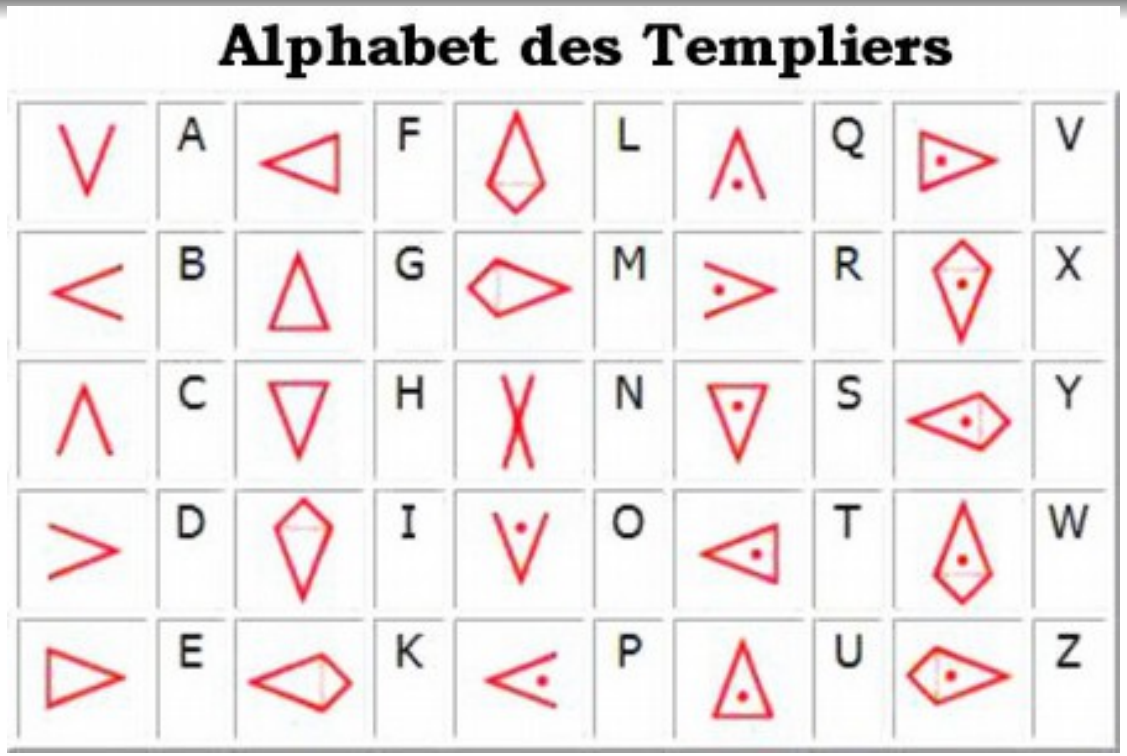

À chaque symbole correspond une lettre de l'alphabet

# Les templiers

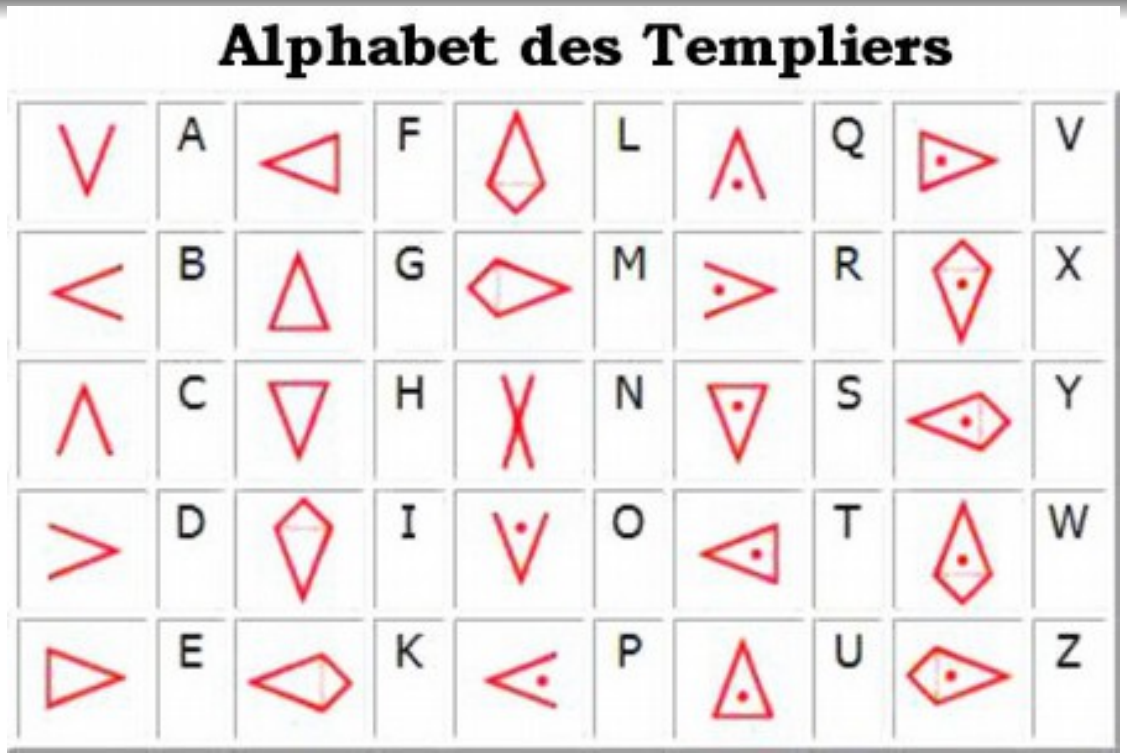


# Les templiers



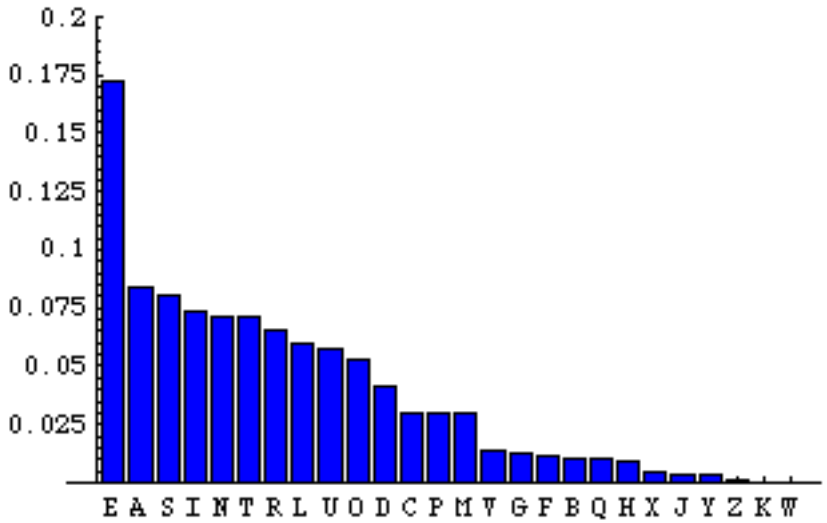

# Les templiers




**A N A L Y S E  D E S  F R E Q U E N C E S**

# Analyse des fréquences

La cryptanalyse est facile grâce à l'utilisation des fréquences des lettres dans l'alphabet français.



# Analyse des fréquences

| | A | B | C | D | E | F | G | H | I | J | K | L | M |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Français** | 9,42 | 1,02 | 2,64 | 3,39 | 15,87 | 0,95 | 1,04 | 0,77 | 8,41 | 0,89 | 0,00 | 5,34 | 3,24 |
| **Anglais** | 8.08 | 1.67 | 3.18 | 3.99 | 12.56 | 2.17 | 1.80 | 5.27 | 7.24 | 0.14 | 0.63 | 4.04 | 2.60 |

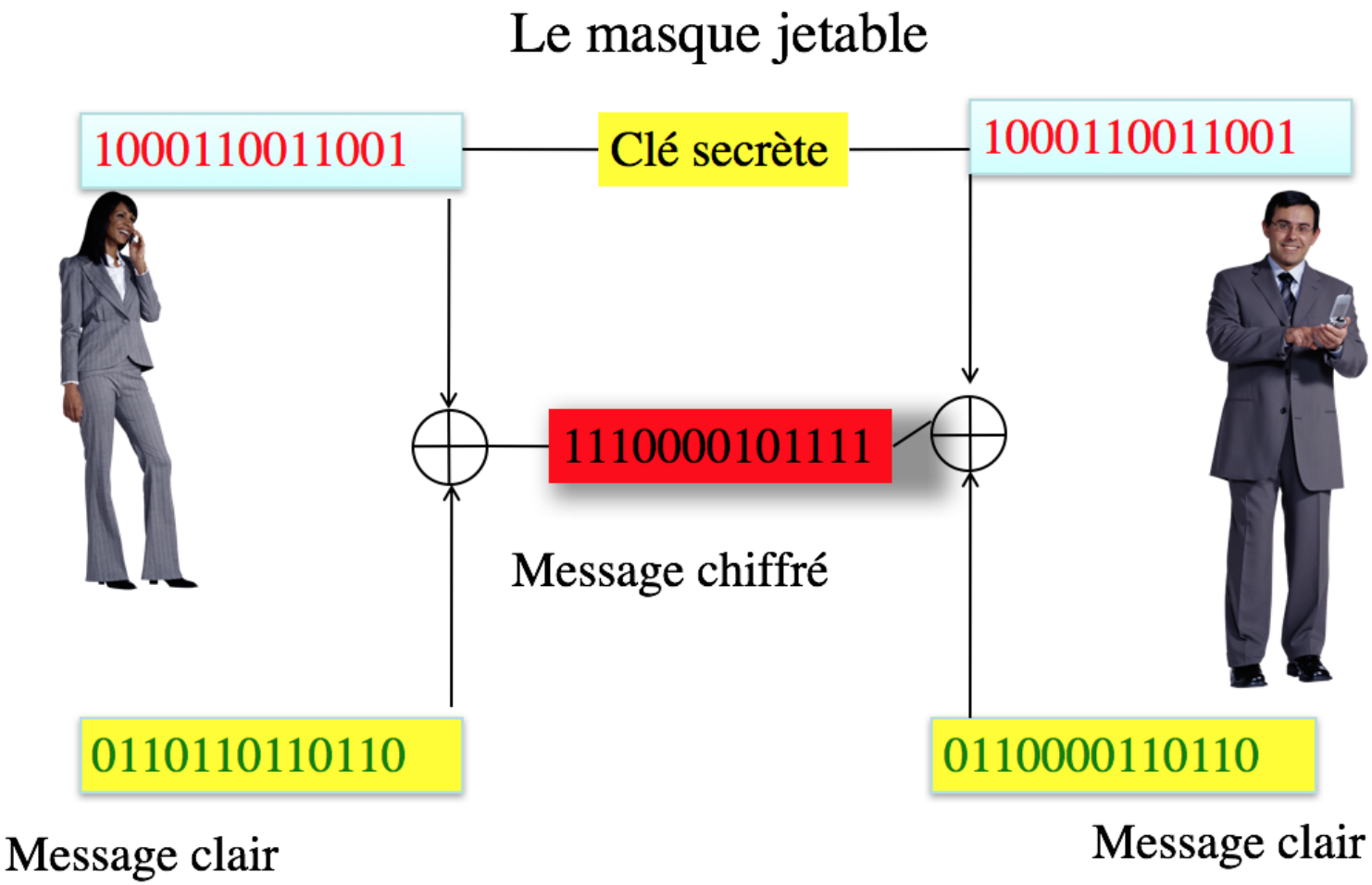
| | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Français** | 7,15 | 5,14 | 2,86 | 1,06 | 6,46 | 7,90 | 7,26 | 6,24 | 2,15 | 0,00 | 0,30 | 0,24 | 0,32 |
| **Anglais** | 7.38 | 7.47 | 1.91 | 0.09 | 6.42 | 6.59 | 9.15 | 2.79 | 1.00 | 1,89 | 0,21 | 1,65 | 0,07 |

# Analyse des fréquences

## Analyse des fréquences, El-Kindi (801-873)


« La façon d'élucider un message crypté, si nous savons dans quelle langue il est écrit, est de nous procurer un autre texte en clair dans la même langue, de la longueur d'un feuillet environ, et de compter alors les apparitions de chaque lettre. Ensuite, nous nous reportons au texte chiffré que nous voulons éclaircir et relevons de même ses symboles. Nous remplaçons le symbole le plus fréquent par la lettre première (la plus fréquente du texte clair), le suivant par la deuxième, le suivant par la troisième, et ainsi de suite jusqu'à ce que nous soyons venus à bout de tous les symboles du cryptogramme à résoudre ».

# Masque jetable



# Le Chiffrement RSA

Le chiffrement dit RSA[1] est basé sur la difficulté de factoriser de grands nombres. Il utilise l'exponentiation modulaire, l'inversion modulaire (ou l'identité de Bézout) et le théorème d'Euler.

[1] Ron Rivest, Adi Shamir et Leonard Adleman en 1977.

# Inverse modulaire

## Théorème

*Soit n un entier naturel non nul. Soit a un entier relatif premier avec n. Alors il existe un entier naturel u tel que :*

$$1 \leq u < n \quad et \quad au \equiv 1 \bmod n.$$

# Petit théorème de Fermat

## Théorème

*Soit a un nombre entier positif et soit p premier ne divisant pas a. Alors :*

$$a^{p-1} \equiv 1 \bmod p$$

**Exemple**
**On a :** $35^{40} \equiv 1 \bmod 41$**.**

# Euler

## Théorème

*Soient $p$ et $q$ deux nombres premiers distincts et soit $n = pq$.*
*Pour tout entier relatif $a$ premier avec $n$, on a :*

$$a^{(p-1)(q-1)} \equiv 1 \bmod n.$$

*En particulier, pour tout entier naturel $k$,*

$$a^{k(p-1)(q-1)+1} \equiv a \bmod n.$$

# Euler

## Théorème

*Soient $p$ et $q$ deux nombres premiers distincts et soit $n = pq$.*
*Pour tout entier relatif $a$ premier avec $n$, on a :*

$$a^{(p-1)(q-1)} \equiv 1 \bmod n.$$

*En particulier, pour tout entier naturel $k$,*

$$a^{k(p-1)(q-1)+1} \equiv a \bmod n.$$

**Exemple**

Soit $p = 373$ et $q = 809$. Ils sont premiers. Soit $n = pq$ et $\varphi(n) = (p-1)(q-1)$. On a
$\varphi(n) = 300576$ et $n = 301757$.
Pour tout entier relatif $a$ et tout nombre naturel $k$,

$$a^{300576k+1} \equiv a \bmod 301757.$$

# Cryptographie à clé publique

- Basée sur l'existence d'opérations dites à sens unique.

# Cryptographie à clé publique

- Basée sur l'existence d'opérations dites à sens unique.
- L'exponentiation modulaire est facile sa réciproque est difficile.

# Cryptographie à clé publique

- Basée sur l'existence d'opérations dites à sens unique.
- L'exponentiation modulaire est facile sa réciproque est difficile.
- Faire un produit c'est facile mais une factorisation c'est difficile.

# RSA : Ronald Rivest, Adi Shamir et Leonard Adleman

Septembre 1977, *A method for obtaining Digital Signatures and Public-key Cryptosystems*

# Principe de chiffrement

**Pour recevoir des messages,** Bob crée ses clés secrète et publique.

- Il choisit deux grands nombres premiers $p$ et $q$ dont il calcule le produit $n$ *(le module du chiffrement).*

# Principe de chiffrement

**Pour recevoir des messages,** Bob crée ses clés secrète et publique.

- Il choisit deux grands nombres premiers $p$ et $q$ dont il calcule le produit $n$ *(le module du chiffrement).*
- Il choisit un nombre $c$ *( clé de chiffrement)* premier avec $\varphi(n) = (p-1)(q-1)$.

# Principe de chiffrement

**Pour recevoir des messages,** Bob crée ses clés secrète et publique.

- Il choisit deux grands nombres premiers $p$ et $q$ dont il calcule le produit $n$ *(le module du chiffrement).*
- Il choisit un nombre $c$ *( clé de chiffrement)* premier avec $\varphi(n) = (p-1)(q-1)$.
- Il calcule $d$ *(clé de déchiffrement)* tel que :

$$dc \equiv 1 \bmod \varphi(n).$$

Ce calcul est rapide car Bob connaît $p$ et $q$.

# Principe de chiffrement

**Pour recevoir des messages,** Bob crée ses clés secrète et publique.

- Il choisit deux grands nombres premiers $p$ et $q$ dont il calcule le produit $n$ *(le module du chiffrement).*
- Il choisit un nombre $c$ *( clé de chiffrement)* premier avec $\varphi(n) = (p-1)(q-1)$.
- Il calcule $d$ *(clé de déchiffrement)* tel que :

$$dc \equiv 1 \bmod \varphi(n).$$

  Ce calcul est rapide car Bob connaît $p$ et $q$.
- Bob garde **secrets** $p$, $q$ et $d$ et rend **publiques** ses *coordonnées* $c$ et $n$.

# Principe de chiffrement

Alice **veut envoyer un message** à Bob.

- Elle regarde dans l'annuaire (publique) et trouve les coordonnées $c$ et $n$ de Bob.

# Principe de chiffrement

Alice **veut envoyer un message** à Bob.

- Elle regarde dans l'annuaire (publique) et trouve les coordonnées $c$ et $n$ de Bob.
- Elle convertit son message en nombres plus petits que $n$ et premiers avec $n$ et les chiffre, en utilisant la clé de chiffrement $c$. Elle procède de la façon suivante : pour un mot, disons $x$, elle calcule

$$y = x^c \bmod n.$$

# Principe de chiffrement

Alice **veut envoyer un message** à Bob.

- Elle regarde dans l'annuaire (publique) et trouve les coordonnées $c$ et $n$ de Bob.
- Elle convertit son message en nombres plus petits que $n$ et premiers avec $n$ et les chiffre, en utilisant la clé de chiffrement $c$. Elle procède de la façon suivante : pour un mot, disons $x$, elle calcule

$$y = x^c \bmod n.$$

- Elle envoie ensuite $y$ à Bob.

# Principe de déchiffrement

Bob **reçoit** $y$. Il utilise sa clé de déchiffrement $d$ pour calculer $y^d \bmod n$. Il obtient $x$ et retrouve ainsi le mot envoyé par Alice. En effet,

$$\begin{aligned} y^d &\equiv (x^c)^d \bmod n \\ &\equiv x^{cd} \bmod n \\ &\equiv x \bmod n \end{aligned}$$

car $cd = 1 + k\varphi(n)$

# Principales références


- P. Dedron et J. Itard, Mathématiques et Mathématiciens, Magnard, Paris 1959
- K. Mainzer et al. Les nombres : leur histoire, leur place et leur rôle de l?antiquité aux recherches actuelles, Vuibert Paris 1998
- S. Singh, Histoire des codes secrets, Springer (Berlin ; Heidelberg ; New York), 1999
- G. Ifrah, Histoire universelle des chiffres, Robert Laffont, Paris 1994

# Sur internet

- http://www.apprendre-en-ligne.net/index.php
- http://pagesperso-orange.fr/therese.eveilleau/
- http://www.picsi.org/accueil.html
- http://fr.wikipedia.org/wiki/Accueil
- http://cryptodox.com/History_of_Cryptography

Merci de votre attention et profitez bien des ateliers !!

Thank you for your attention and enjoy the workshops !!

Vielen Dank für Ihre Aufmerksamkeit and profitieren von den Werkstätten !!