UNIVERSITÉ PARIS 8 VINCENNES-SAINT-DENIS

Principes fondamentaux de la cryptographie

Amal BOURMADA
Amal.bourmada@univ-paris8.fr
Master 1 – Informatique
Semestre 2

Plan

1. Terminologie
2. Objectifs de la cryptographie
3. Chiffrement / Déchiffrement
4. Chiffrement Symétrique
5. Chiffrement Asymétrique

Terminologie

- **La Cryptologie** : Cela signifie la "science du secret". La cryptologie se partage entre la *cryptographie* et la *cryptanalyse* ;
- Le mot « **Cryptographie** » est composé des mots grecques :

CRYPTO = caché

GRAPHY = écrire

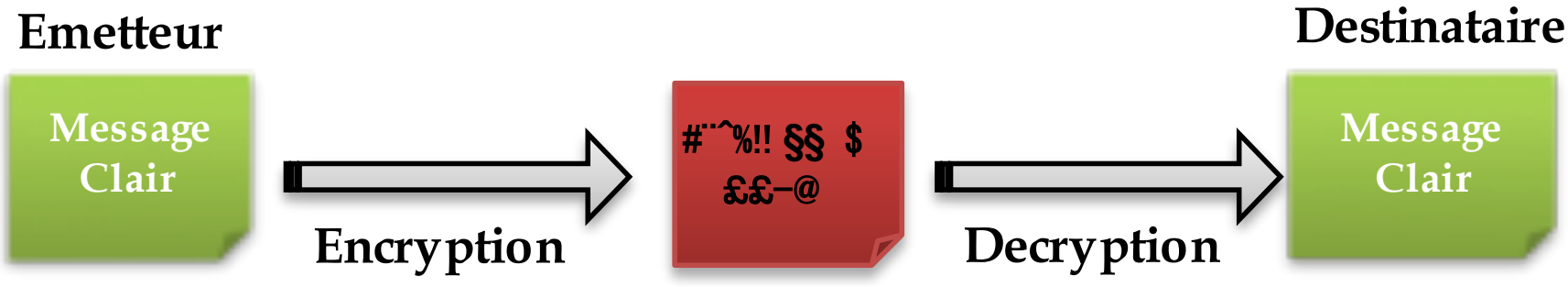
  - C'est donc l'art de l'écriture secrète.
  - C'est une science permettant de préserver la confidentialité des échanges.

Terminologie

La Cryptanalyse

La cryptanalyse est l'art de décrypter des messages chiffrés.

Rendre le message compréhensible.



Terminologie

Plus précisément,

1 Cryptographie: étude et conception des procédés de chiffrement des informations ;

2 Cryptanalyse : Analyse des textes chiffrés pour retrouver des informations dissimulées, Analyse des procédés de chiffrement afin d'en découvrir les failles de sécurité.

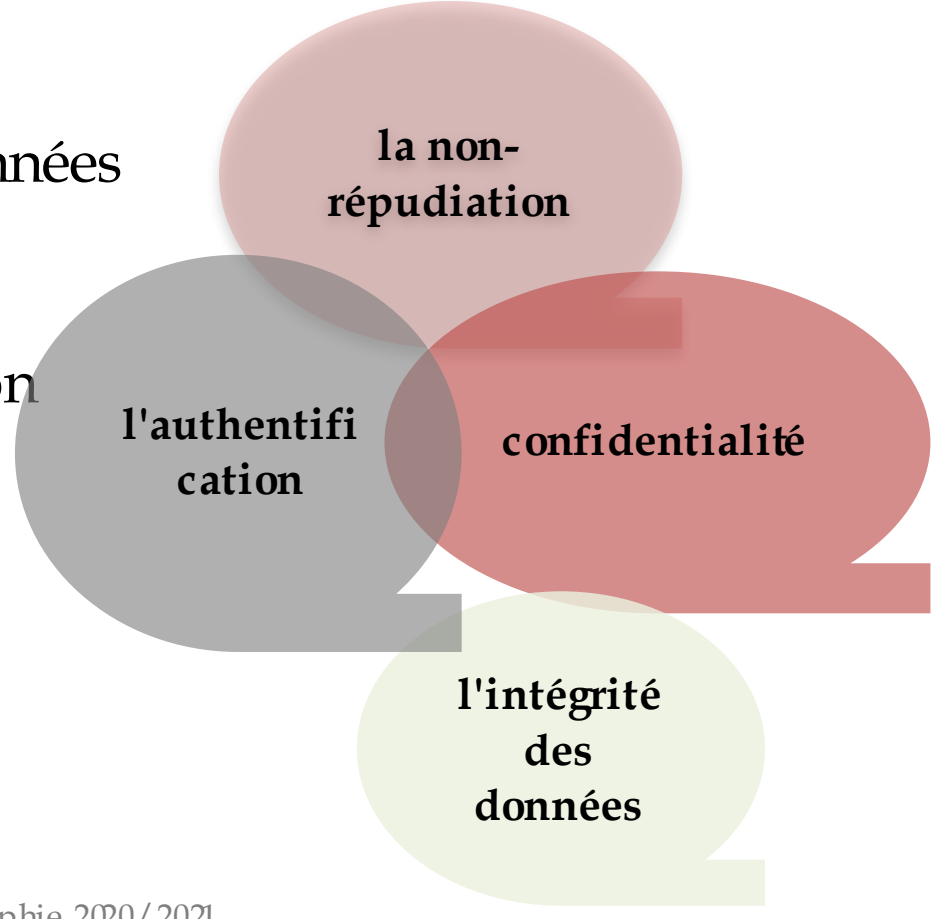
Terminologie

- Un système de chiffrement s'appelle un **cryptosystème** ;
- Un **cryptographe** est une personne qui conçoit des cryptosystèmes ;
- Un **cryptanaliste** est une personne qui tente de casser les cryptosystèmes.
- **Signature s :** Chaine de caractères associées à un message donné (et aussi possiblement à une entité) et le caractérisant.

Objectifs de la cryptographie

Parmi les objectifs de la cryptographie :

- Garantir la confidentialité
- Vérifier l'intégrité des données
- Gérer l'authentification
- Assurer la non-répudiation



Chiffrement / Déchiffrement

Texte (ou message) clair : Information qu'Alice souhaite transmettre à Bob. Par exemple, un texte en français ou des données numériques;

Chiffrement/déchiffrement

Le ***chiffrement*** est une transformation cryptographique qui transforme un message clair en un message inintelligible (dit message chiffré), afin de cacher la signification du message original aux tierces entités non autorisées à l'utiliser ou le lire.

Le ***déchiffrement*** est l'opération qui permet de restaurer le message original à partir du message chiffré.

Chiffrement / Déchiffrement

Chiffrement : Processus de transformation d'un message clair ***M*** de façon à le rendre incompréhensible (sauf aux interlocuteurs légitimes). Il est basé sur une fonction de chiffrement ***E*** qui permet de générer un message chiffré:

$$C = E(M)$$

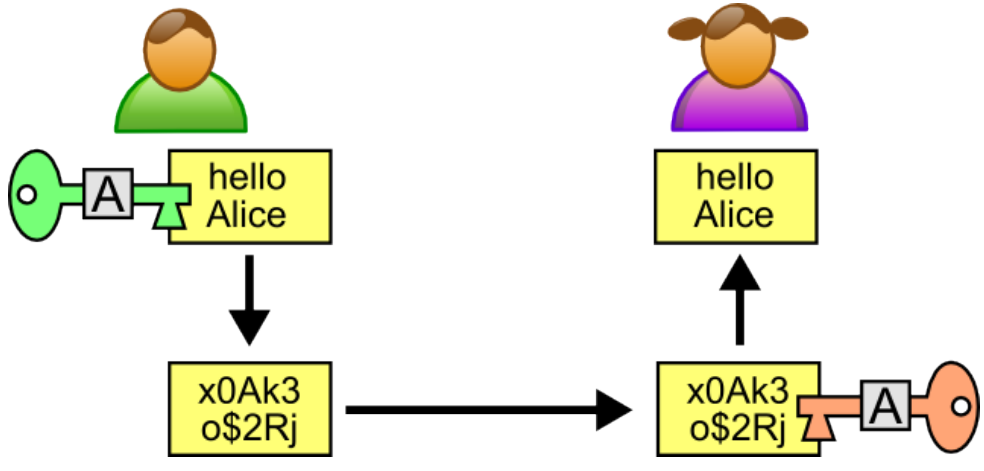
Déchiffrement : Il est basé sur une fonction de déchiffrement ***D*** telle que si ***C*** est le message chiffré correspondant au message clair ***M,*** alors :

$$D(C) = M$$

Chiffrement / Déchiffrement

Clé de chiffrement

- L'habilité de maintenir un message chiffré secret, repose non pas sur l'algorithme de chiffrement (qui est largement connu), mais sur une information secrète dite CLE qui doit être utilisée avec l'algorithme pour produire le message chiffré.



Chiffrement / Déchiffrement

En pratique, et pour plus de sécurité, les fonctions E et D sont paramétrées par des clefs K_e et K_d :

K_e : est la clef de chiffrement
K_d : est la clef de déchiffrement.

Dire que E et D sont paramétrées signifie qu'elles dépendent de la clef. On note cette dépendance E_{Ke} ou $D_{Kd.}$ Pour M un message clair, on doit avoir:

$$\begin{cases} E_{Ke}(M) = C, \\ D_{Kd}(C) = M. \end{cases}$$

Chiffrement / Déchiffrement

Selon que la clé utilisée pour le chiffrement et le déchiffrement est la même ou pas, on parle de système cryptographique :

Symétrique

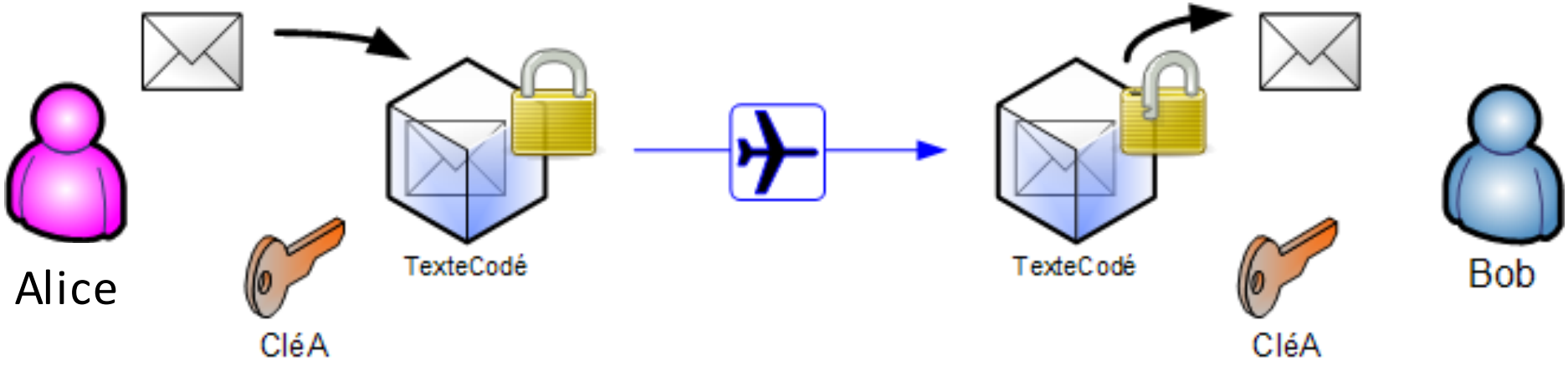
ou

Asymétrique.

Chiffrement Symétrique

Chiffrement symétrique

- Une même clé est partagée entre l'émetteur et le récepteur.
- Cette clé dite symétrique est utilisée par l'émetteur pour chiffrer le message et par le récepteur pour le déchiffrer en utilisant un ***algorithme de chiffrement symétrique***.



Chiffrement Symétrique

Algorithmes de Chiffrement symétrique

Quelques exemples d'algorithmes symétriques

1. Le chiffrement de césar

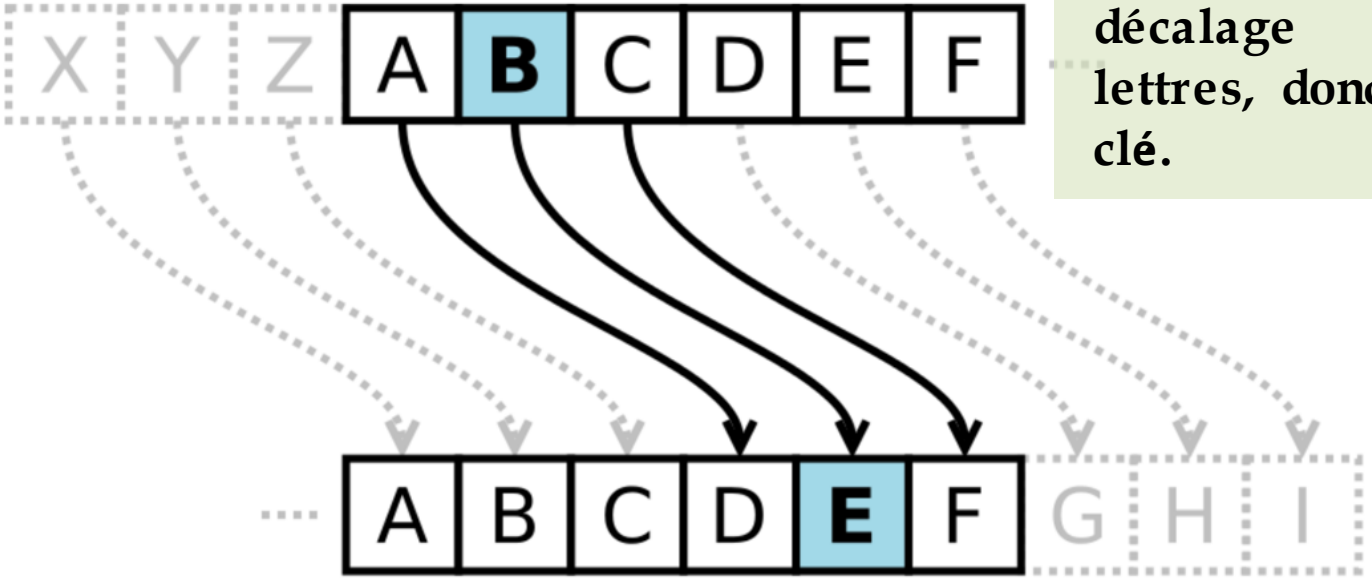
- Le chiffrement par décalage, aussi connu comme le chiffre de César ou le code de César, est une méthode de chiffrement très simple utilisée par Jules César dans ses correspondances secrètes (ce qui explique le nom « chiffre de César »).
- La méthode de cryptographie la plus ancienne communément admise par l'histoire.
- Il consiste en une substitution mono-alphabétique, où la substitution est définie par un décalage de lettres.

Chiffrement Symétrique

Algorithmes de Chiffrement symétrique

Quelques exemples d'algorithmes symétriques

1. Le chiffrement de césar



Jules César utilisait systématiquement le décalage de trois lettres, donc la même clé.

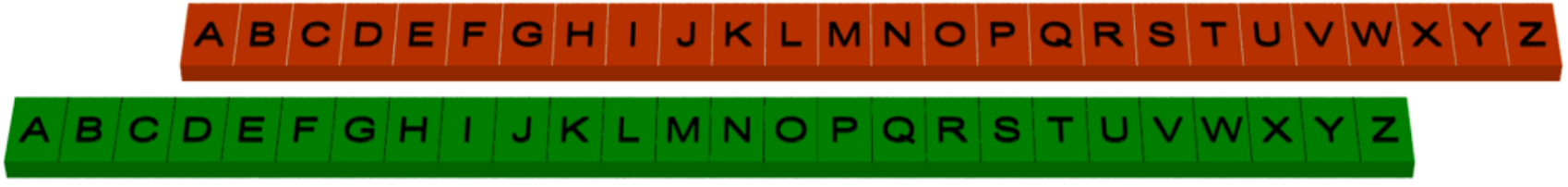
Chiffrement Symétrique

Algorithmes de Chiffrement symétrique

1. Le chiffrement de césar

Jules César a-t-il vraiment prononcé la célèbre phrase :

DOHD MDFWD HVW

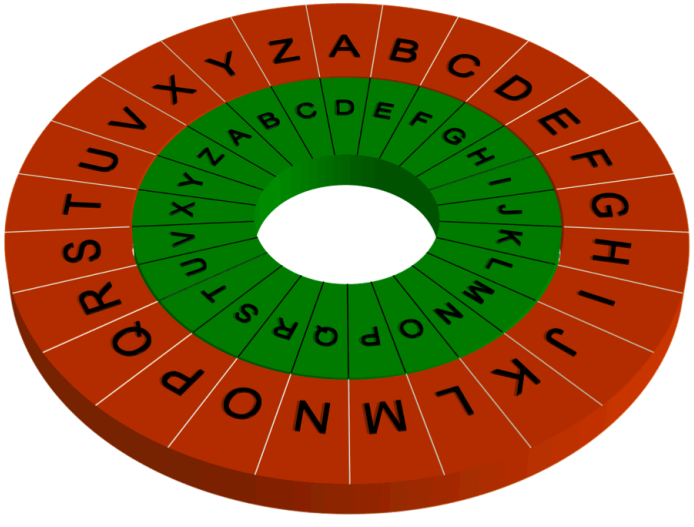


Chiffrement Symétrique

Algorithmes de Chiffrement symétrique

1. Le chiffrement de césar

Le décalage de lettre est un ***décalage circulaire*** sur les lettres de l'alphabet.



Et la célèbre phrase de César est :

ALEA JACTA EST

qui traduite du latin donne « Les dés sont jetés ».

Chiffrement Symétrique

1. Le chiffrement de César

1.1 Des chiffres et des lettres

Nous associons à chacune des 26 lettres de A à Z un nombre de 0 à 25. En termes mathématiques, nous définissons une bijection :

$$f : \{A, B, C, \ldots, Z\} \longrightarrow \{0, 1, 2, \ldots, 25\}$$

par

$$A \longmapsto 0 \quad B \longmapsto 1 \quad C \longmapsto 2 \quad \ldots \quad Z \longmapsto 25$$

Ainsi "**A L E A**" devient "**0 11 4 0**".

Pour cela, rappelons la notion de congruence et l'ensemble $/26$.

Chiffrement Symétrique

1. Le chiffrement de César

1.2 Modulo

Soit $n >= 2$ un entier fixé.

Définition 1.
On dit que *a est congru à b modulo n*, si n divise $b-a$.
On note alors $a \equiv b \pmod{n}$.

Pour nous: $n=26$.

Exemple: $28 \equiv 2 \pmod{26}$, car $28-2$ est bien divisible par 26.
De même $85=3\times26+7$ donc $85 \equiv 7 \pmod{26}$.

On note $\mathbb{Z}/26\mathbb{Z}$ l'ensemble de tous les éléments de modulo 26.

Chiffrement Symétrique

1. Le chiffrement de César

1.3 Chiffrer et déchiffrer

Le chiffrement de César est simplement une addition dans Z /26 !

$$C_k : \begin{cases} \mathbb{Z}/26\mathbb{Z} & \longrightarrow & \mathbb{Z}/26\mathbb{Z} \\ x & \longmapsto & x+k \end{cases}$$

K est le décalage (par exemple ***k = 3*** dans l'exemple de César) et définissons la ***fonction de chiffrement de César de décalage*** *k*

Chiffrement Symétrique

1. Le chiffrement de César

1.3 Chiffrer et déchiffrer

Exemple:

pour $k = 3$:

$C_3(0) = 3, C_3(1) = 4 \ldots$

Pour déchiffrer, rien de plus simple ! Il suffit d'aller dans l'autre sens, c'est-à-dire ici de soustraire.

Chiffrement Symétrique

1. Le chiffrement de César

1.3 Chiffrer et déchiffrer

La **fonction de déchiffrement de César de décalage** k est:

$$D_k : \begin{cases} \mathbb{Z}/26\mathbb{Z} & \longrightarrow & \mathbb{Z}/26\mathbb{Z} \\ x & \longmapsto & x-k \end{cases}$$

En effet, si 1 a été chiffré en 4, par la fonction C_3 alors $D_3(4) = 4 - 3 = 1$.

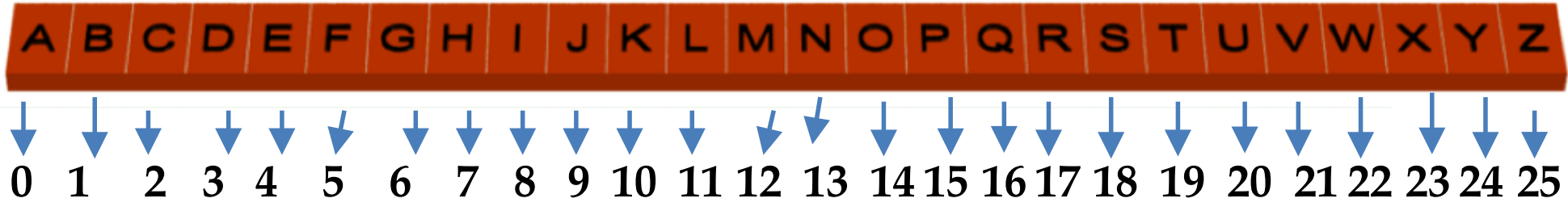
D_k est la bijection réciproque de C_k, ce qui implique que pour tout $x \in \mathbb{Z}/26\mathbb{Z}$

$$D_k\big(C_k(x)\big) = x$$

Chiffrement Symétrique

1. Le chiffrement de César

1.3 Chiffrer et déchiffrer



Supposons: K= 11

Chiffrement Symétrique

1. Le chiffrement de César

1.3 Chiffrer et déchiffrer

- Alice veut envoyer des messages secrets à Bob.
- Par exemple $k = 11$.
- Alice veut envoyer le message "**COUCOU**" à Bruno.
- Elle transforme "**COUCOU**" en "**2 14 20 2 14 20**".
- Elle applique la fonction de chiffrement $C_{11}(x) = x + 11$ à chacun des nombres :

  "**13 25 5 13 25 5**" ce qui correspond au mot crypté "**NZFNZF**".
- Elle transmet le mot crypté à Bruno, qui selon le même principe applique la fonction de déchiffrement $D_{11}(x) = x - 11$

Chiffrement Symétrique

1. Le chiffrement de César

1.4 Attaque

- Il est clair que ce chiffrement de César est d'une sécurité très faible.
- Si Alice envoie un message secret à Bob et que Chloé intercepte ce message, il sera facile pour Chloé de le décrypter même si elle ne connait pas la clé secrète k.
- L'attaque la plus simple pour Chloé est de tester ce que donne chacune des 26 combinaisons possibles et de reconnaître parmi ces combinaisons laquelle donne un message compréhensible.

Chiffrement Symétrique

Algorithmes de Chiffrement symétrique

2. Le chiffrement de Vigenère

- Le chiffrement de César présente une sécurité très faible, l'espace des clés est trop petit :  il y a seulement 26 clés possibles.
- Un message chiffré est attaqué en testant toutes les clés à la main.
- Il est basé sur les 26 lettres de l'alphabet latin en réalisant une substitution cyclique des symboles du texte clair.

Chiffrement Symétrique

2. Le chiffrement de Vigenère

2.1 Le principe

- Ce chiffrement introduit la notion de clé
- La clé secrète est une chaîne de caractères (mieux si aléatoires);
- La longueur est secrète. Par exemple AXFRE est une clé de longueur 5;
- Le texte clair est préalablement réduit aux seules lettres de l'alphabet (tous les espaces, accents, etc. sont éliminés).

Chiffrement Symétrique

2. Le chiffrement de Vigenère

2.2 La table de Vigenère

- L'outil indispensable du chiffrement de Vigenère est : **" La table de Vigenère »**

Lettre en clair

La Clé utilisée	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

UNIVERSITÉ PARIS 8 VINCENNES-SAINT-DENIS

2. Le chiffrement de Vigenère

2.2 La table de Vigenère

- Pour chaque lettre en clair, on sélectionne la colonne correspondante.
- Pour une lettre de la clé on sélectionne la ligne adéquate,
- Puis au croisement de la ligne et de la colonne on trouve la lettre codée.
- La lettre de la clé est à prendre dans l'ordre dans laquelle elle se présente et on répète la clé en boucle autant que nécessaire.

Chiffrement Symétrique

2. Le chiffrement de Vigenère

2.3 Exemple

On veut coder le texte "CRYPTOGRAPHIE DE VIGENERE" avec la clé "MATHWEB". On commence par écrire la clef sous le texte à coder :

C	R	Y	P	T	O	G	R	A	P	H	I	E		D	E		V	I	G	E	N	E	R	E
M	A	T	H	W	E	B	M	A	T	H	W	E		B	M		A	T	H	W	E	B	M	A

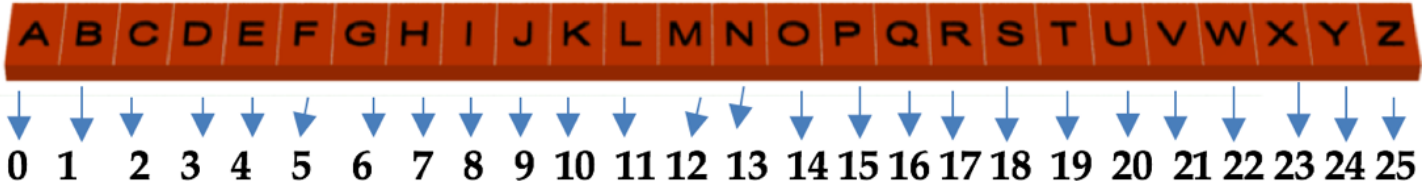
Colonne **C**, ligne **M**, on obtient la lettre **O**
Colonne **R**, ligne **A**, on obtient la lettre **R**
…

Résultat: → **ORRWPSHDAIOEI EQ VBNARFDE**

Chiffrement Symétrique

2. Le chiffrement de Vigenère

2.4 Principe Mathématique



- La transformation lettre par lettre se formalise simplement par :

Codé = (Texte + clé) mod 26

- Il suffit d'effectuer l'addition des deux caractères puis de trouver le numéro correspondant à la lettre codée,
- Notre alphabet étant circulaire (après Z on a A),
- la congruence nous assure que notre résultat sera compris entre 0 et 25.

Chiffrement Symétrique

2. Le chiffrement de Vigenère

2.4 Attaque

- Le cryptosystème de Vigenère a longtemps été considéré incassable.
- Cependant, sa cryptanalyse est très aisée à l'aide des ordinateurs.
- En supposant la longueur **n** de la clé connue, un message peut être décrypté rapidement.
- Pour déterminer la taille de la clé, on peut utiliser le test de Kasiski ou une technique basée sur l'indice de coïncidence.