



Cybersécurité - Cours 3: La cryptographie

SIO - Bloc 1 - SMDSI

M. SPINA



Sommaire

1. Introduction
2. Définitions
3. Le chiffrement
 - a. son fonctionnement
 - b. la chronologie des méthodes
 - c. les méthodes courantes
4. Méthodes par substitution
 - a. Le chiffre de César
 - b. Le chiffre de Vigenère
 - c. La méthode Turing

Introduction

On a vu que la communication au sein d'une entreprise pouvait représenter une véritable faille.

Depuis l'Égypte ancienne, l'homme veut pouvoir échanger des informations de façon confidentielle.

C'est pourquoi, il a cherché et trouvé des techniques pour protéger l'accès à l'information.





Introduction

Il existe de nombreux domaines où ce besoin est vital :

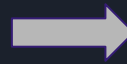
- **militaire** (sur un champ de bataille ou pour protéger l'accès à l'arme nucléaire)
- **commercial** (protection de secrets industriels)
- **bancaire** (protection des informations liées à une transaction financière)
- **de la vie privée** (protection des relations entre les personnes)
- **diplomatique** (le fameux « téléphone rouge » entre Etats-Unis et Union soviétique)
- etc.

Introduction

“Au service du gouvernement Britannique, il a percé le secret de la célèbre machine de cryptage allemande Enigma, réputée inviolable.”



Allan Turing, mathématicien, cryptologue





Définitions

La **Cryptologie** → signifie littéralement « **science du secret** », elle comprend:

- la **cryptographie**: l'étude des écritures secrètes,
- la **cryptanalyse**: le déchiffrement d'un message sans en avoir la clé
- et la **stéganographie**: l'art de la dissimulation

La **Cryptographie** → sert à **assurer la protection de messages**

- elle assure leur intégrité, authenticité et leur confidentialité

Le **Chiffrement** → **procédé de la cryptographie (méthode)**

- permet de rendre incompréhensible un document sauf si on possède la clé de (dé)chiffrement

Définitions

NE PAS CONFONDRE déchiffrement >< décryptage:

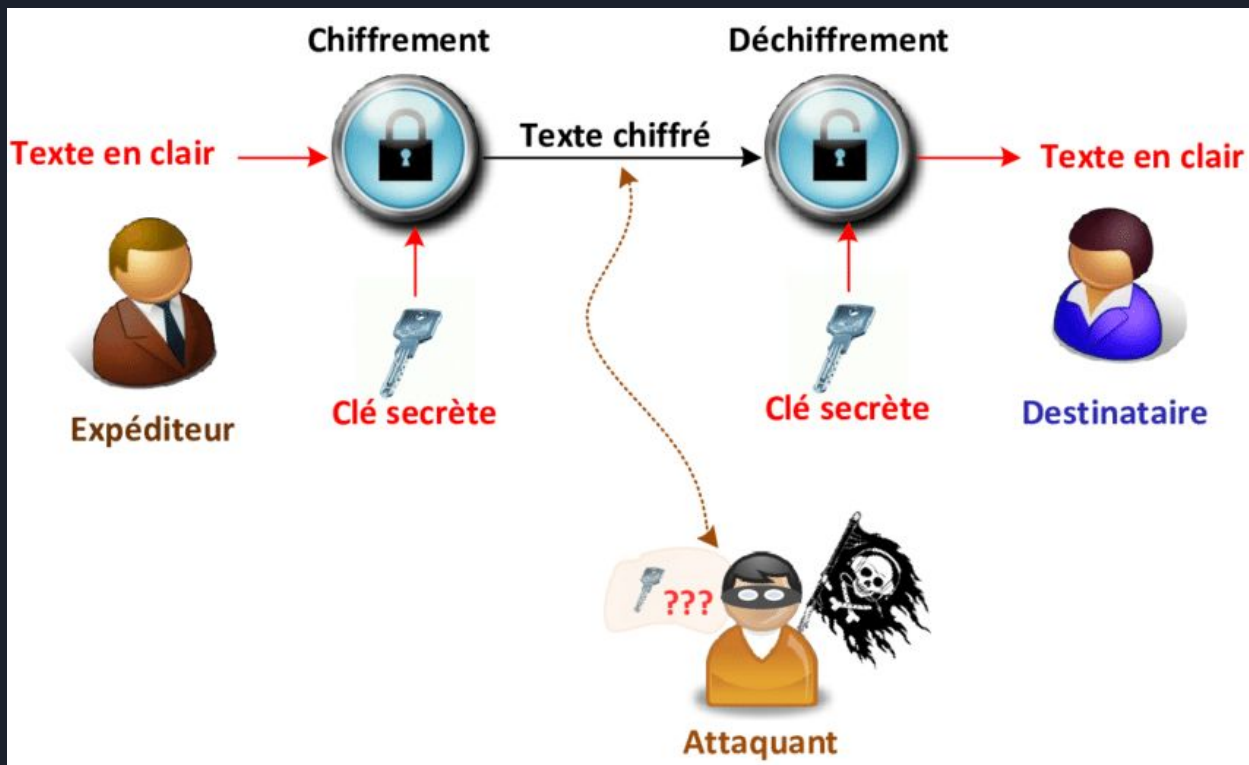
Déchiffrement → déchiffrer un message en possédant la clé de (dé)chiffrement



Décryptage → méthode pour déchiffrer un message sans posséder la clé de (dé)chiffrement



Le chiffrement: fonctionnement



Le chiffrement: chronologie des méthodes

Ve siècle avant JC	Ier siècle avant JC	1586
Les Spartiates	Jules César	Blaise de Vigenère (1523-1596), cryptographe français
Un <u>bâton de bois</u> autour duquel s'enroule une bande de cuir sur laquelle est écrit le message : il faut avoir un 2ème bâton pour déchiffrer	<u>Méthode de substitution:</u> décaler les lettres de l'alphabet d'un nombre n de cases (si $n=3$, A devient D, etc.): il faut connaître " n " pour pouvoir déchiffrer	<u>Méthode de substitution</u> <u>polyalphabétique</u> : une même lettre peut, suivant sa position dans le message, être remplacée par des lettres différentes. Technique la plus utilisée jusqu'au XIXe siècle.

Le chiffrement: chronologie des méthodes

1942	1977	2000
Alan Turing (1912-1954) mathématicien britannique	Adi Shamir, Roland Rivest et Leonard Adleman	Vincent Rijmen et Joan Daemen
fabrique un système capable de décrypter la machine Enigma utilisée par l'armée allemande pour crypter ses messages.	inventent l'algorithme RSA, 1er système de cryptographie associant une clef publique et une clef privée. Utilisée aujourd'hui pour systèmes de paiement du commerce électronique.	créent l'algorithme AES, qui est à ce jour le plus solide système de cryptographie symétrique : pour en venir à bout, il faut effectuer 10^{77} opérations.



Le chiffrement: méthodes courantes

Ces méthodes ont évolué à cause, ou plutôt grâce à leur faible niveau de sécurité. On peut aujourd'hui les répertorier en deux grandes familles de chiffrement:

- **par substitution**
- **par transposition (permutation)**

Le chiffrement: mise au point

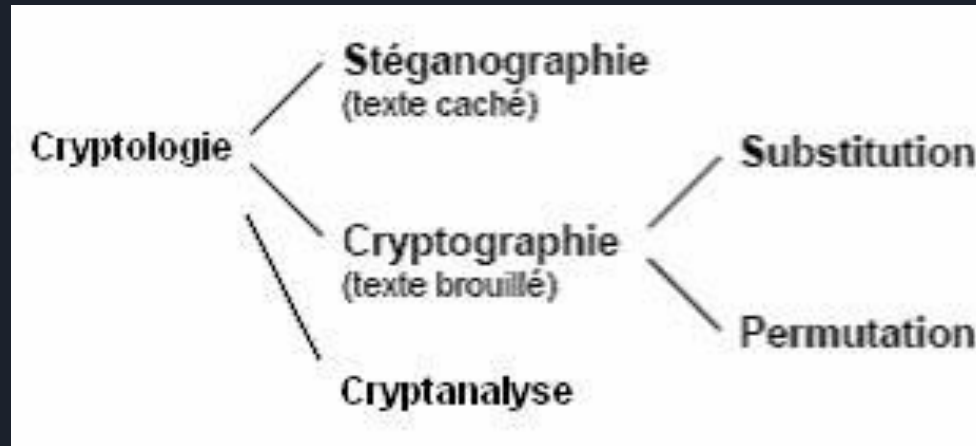


Schéma représentant les familles de la cryptologie



Le chiffrement: par substitution

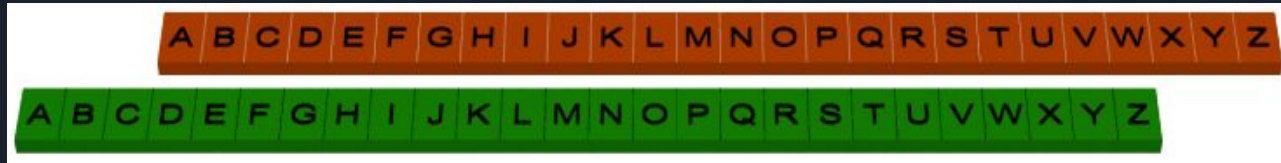
Les méthodes de chiffrement par substitution que nous allons étudier sont:

- **le chiffre de César**
- **le chiffrement RSA (introduction de clé secrète)**

Le chiffre de César

A l'époque, pour ses communications importantes à son armée, César cryptait ses messages à l'aide d'une technique simple: le décalage des lettres de l'alphabet → **méthode de substitution monoalphabétique**

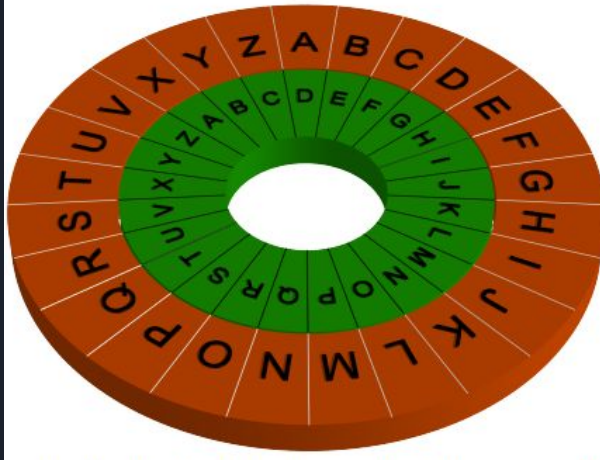
→ A devient D, B devient E, C devient F, etc.



Exemple: Déchiffrer ce message: **DOHD MDFWD HVW**

Le chiffre de César

Réponse **ALEA JACTA EST** qui signifie “Les dés sont jetés” en latin



Inconvénient: sécurité faible
→ **nombre de clés limité à 26**

On peut attaquer un message
chiffré en testant toutes les clés
à la main

“Avez-vous une proposition d’amélioration ?”



Le chiffre de César: une amélioration ?

Au lieu de faire correspondre circulairement les lettres, on associe maintenant à chaque lettre une autre lettre (sans ordre fixe ou règle générale).

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

Exemple: Déchiffrer ce message:

XGKX DR SX OFV XGKX GXWWX XVG WF ZRXVGPDS



Le chiffre de César: une amélioration ?

Réponse:

ETRE OU NE PAS ETRE TELLE EST LA QUESTION

Avantage: l'espace des clés est gigantesque et il n'est plus question d'énumérer toutes les possibilités.

Inconvénients: la clé à retenir est beaucoup plus longue, puisqu'il faut partager la clé constituée des 26 lettres.

De plus, chaque lettre aura une et une seule lettre correspondante.

Mais surtout, ce protocole de chiffrement est lui aussi assez simple à « craquer ».



Le chiffre de Vigenère

Cette méthode introduit la notion de **chiffrement polyalphabétique par bloc**, le texte clair est chiffré à l'aide d'une clé constituée de ***n*** nombres.

Exemple:

CE TEXTE EST CHIFFRE PAR VIGENERE

on simplifie par

CETEXTEESTCHIFFREPARVIGENERE

on choisit la clé ***k* = CHIFFRE (3,8,9,6,6,18,5)**



Le chiffre de Vigenère

Exemple: cela nous donne

CETEXTEESTCHIFFREPARVIGENERE

CHIFFRECHIFFRECHIFFRECHIFFRE

= FMCKDLJHACINAKIZNVGJALONTKJJ

Analyse: On remplace chaque lettre par une lettre différente

→ nombre de possibilités immense: $26! * \text{nombre_de_lettres}$



Analyse des deux méthodes

Inconvénients:

- chiffre de César: k de longueur 1
- chiffre de Vigenère: k de longueur aléatoire mais se répète
- l'alphabet est une suite fixe de 26 lettres
- avec une clé k , on peut chiffrer et déchiffrer

→ ce qui fait qu'une attaque statistique est toujours possible.



Le chiffrement à clé asymétrique

Cette méthode consiste à créer une fonction à sens unique :

- on peut facilement chiffrer un message à l'aide d'une clé
- MAIS difficilement le déchiffrer sans avoir la **deuxième clé**

Ainsi, cette méthode est basée sur celle des systèmes de cryptage symétriques, où une même clé peut chiffrer et déchiffrer, sauf que celle-ci ajoute une clé supplémentaire pour déchiffrer.



Le chiffrement RSA

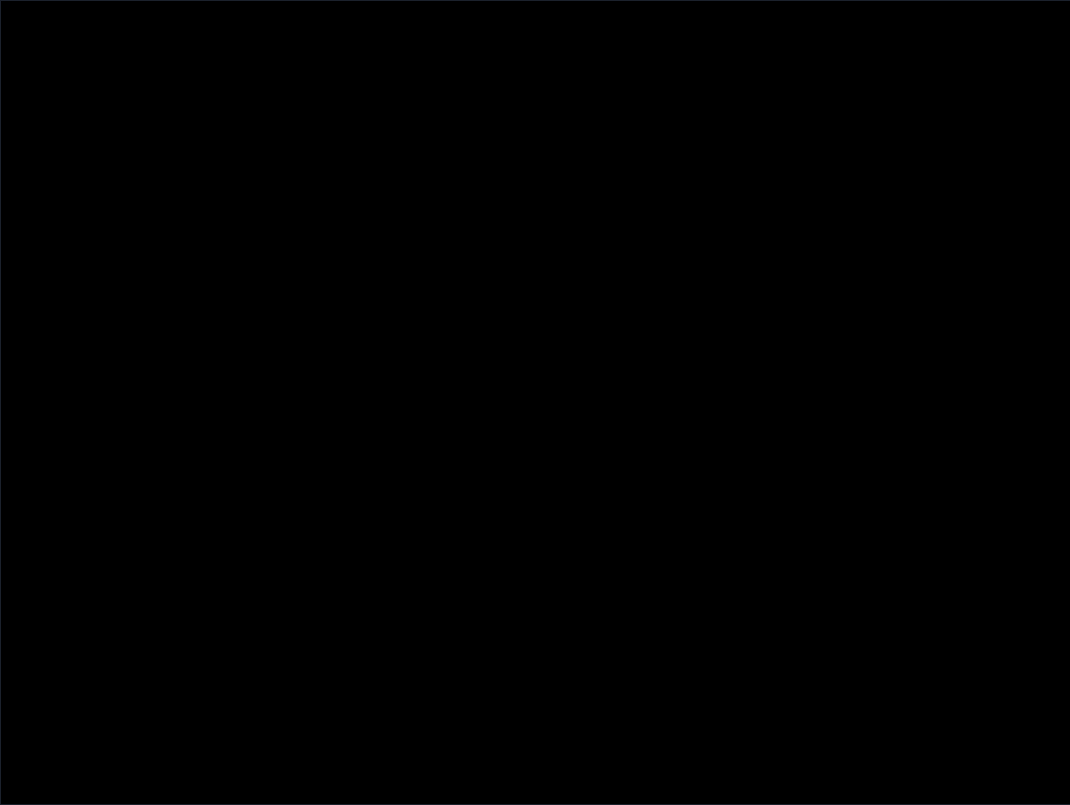
En 1977, Roland Rivest, Adi Shamir et Leonard Adleman inventent l'algorithme RSA (portant leurs initiales), 1er système de cryptographie associant une clef publique et une clef privée.

Cette méthode **renforce le niveau de sécurité du cryptage** et vient donc substituer la méthode de chiffrement à clés symétriques.

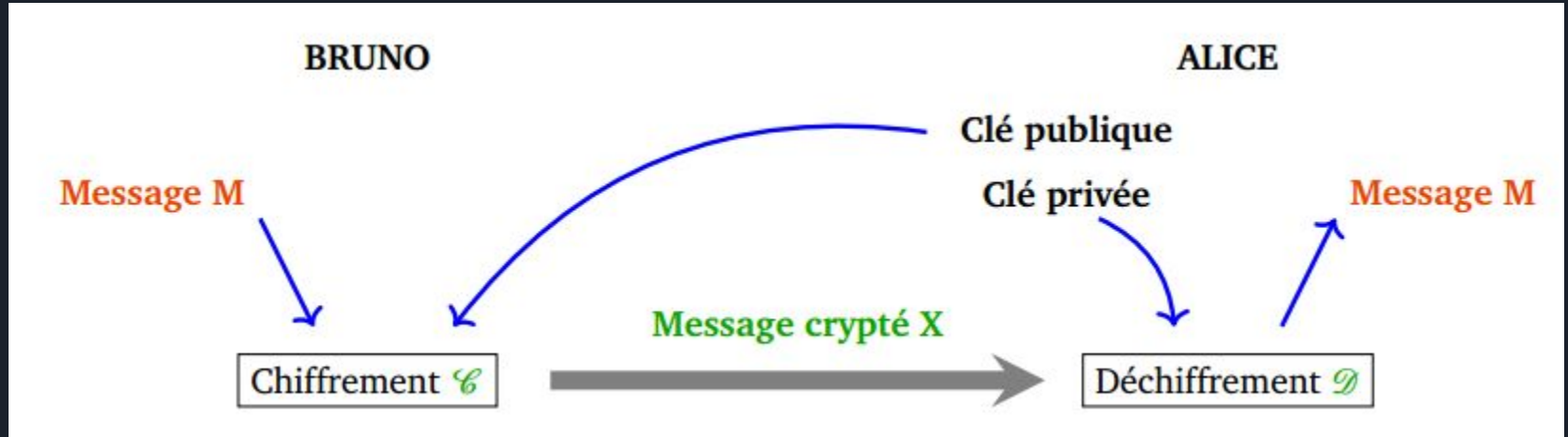


Le chiffrement RSA: Fonctionnement

Vidéo de
présentation.



Le chiffrement RSA: Fonctionnement





Le chiffrement RSA: Fonctionnement

Forme imagée:

Si Bruno veut envoyer un message secret à Alice, le processus se décompose ainsi :

- 1) Alice prépare deux clés: une **clé publique** et une **clé privée**,
- 2) Bruno utilise la clé publique d'Alice pour **chiffrer son message**,
- 3) Alice reçoit le message chiffré et le **déchiffre grâce à sa clé privée**.



Le chiffrement RSA: En pratique

Il existe plusieurs techniques pour créer une paire de clés. Sous Linux, les plus connues sont PGP et OpenSSL.

<http://www.sharevb.net/IMG/pdf/ssl>

<https://www.eila.univ-paris-diderot.fr/sysadmin/securite/ca/chiffrement>

http://cayrel.net/IMG/pdf/PKI_PGP_OpenSSL.pdf