# Sécurité Informatique

## Chapitre III : Introduction à la cryptographie

# Plan du cours

1. Terminologie
2. Définition et Historique
3. Service de la cryptographie
4. Cryptographie Classique
5. Cryptographie Moderne
6. Signature électronique
7. Certificat
8. Mises en œuvre concrètes
9. Cryptanalyse

# Terminologie

## Définitions des termes courants de cryptologie

**Cryptologie**

Science des messages secrets. Elle se décompose en deux disciplines: la **cryptographie** et la **cryptanalyse**.

Art de transformer un message clair en un message inintelligible par celui qui ne possède pas les clefs de chiffrement.

Art d'analyser un message **chiffré** afin de le **décrypter**.

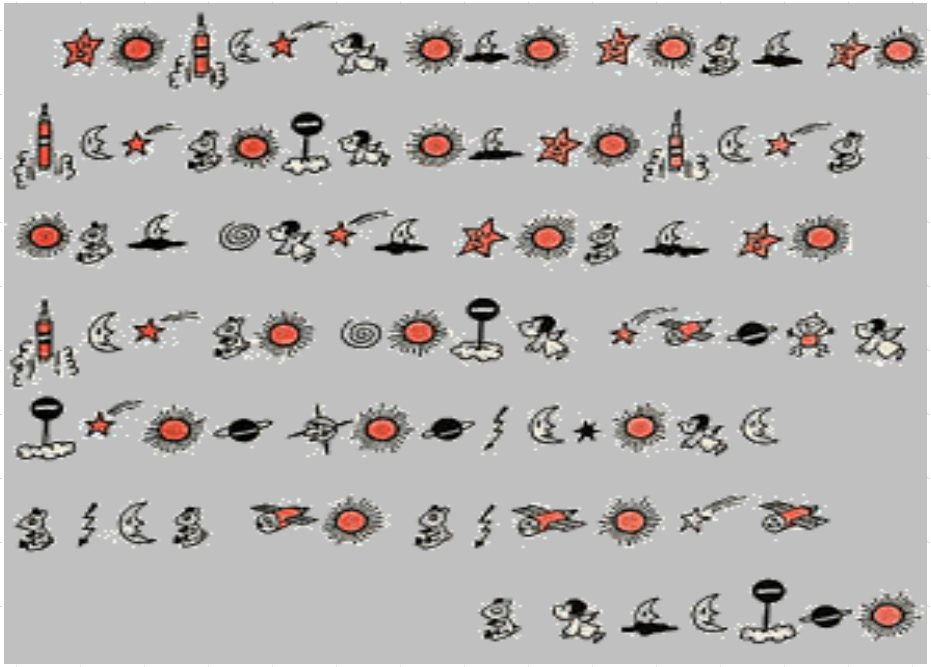
**Cruptos** ($\chi\rho\upsilon\pi\tau o\sigma$) : caché, dissimulé

**Graphein** ($\gamma\rho\alpha\phi\epsilon\iota\nu$) : écrire

# Définitions des termes courants de cryptologie

**Chiffré**

Ensemble de procédés et ensemble de symboles (lettres, nombres, signes, etc.) employés pour remplacer les **lettres** du message à chiffrer.

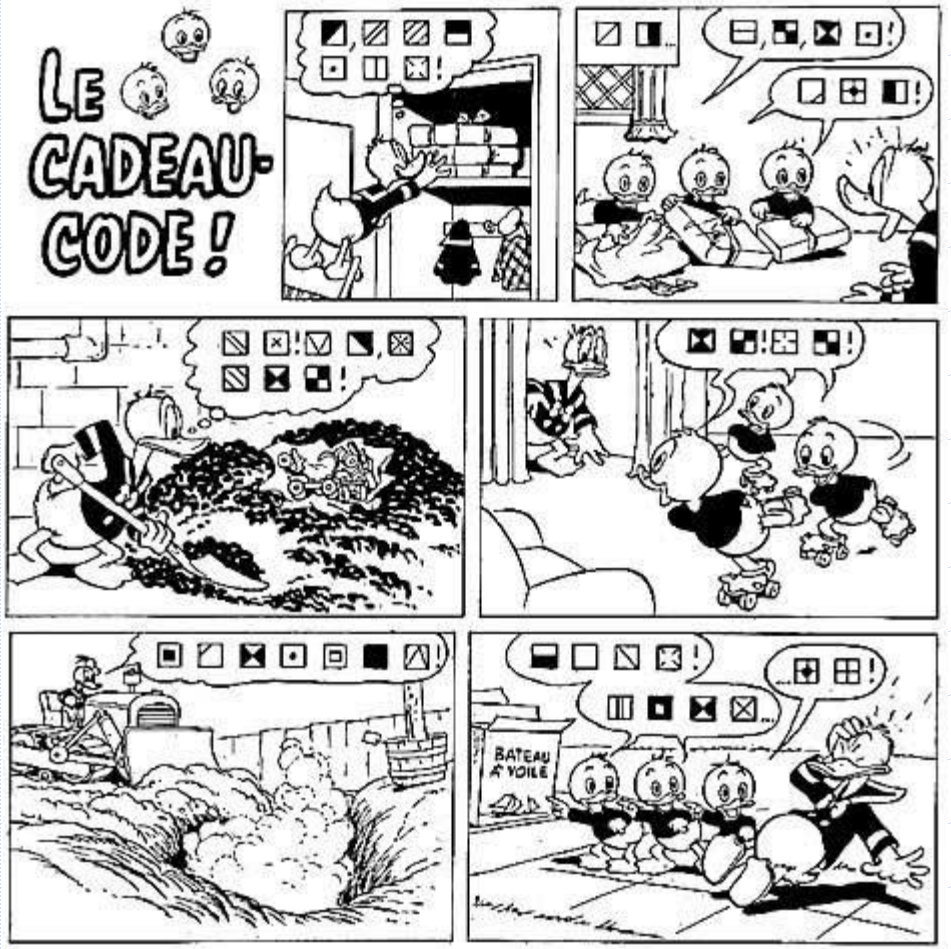


**Indice***:* le dernier mot est une planète du système solaire

# Définitions des termes courants de cryptologie

**Code**

Ensemble de procédés et ensemble de symboles (lettres, nombres, signes, etc.) employés pour remplacer les **mots** du message à coder

# Définitions des termes courants de cryptologie

**Déchiffrement**

Opération inverse du chiffrement, i.e. obtenir la version originale d'un message qui a été précédemment chiffré **en connaissant la méthode de chiffrement et les clefs (contrairement au décryptement)**.

**Décryptement**

Restauration des données qui avaient été chiffrées à leur état premier ("en clair"), **sans disposer des clefs** théoriquement nécessaires.

# Définitions des termes courants de cryptologie

## Stéganographie

Branche particulière de la cryptographie qui consiste non pas à rendre le message inintelligible, mais à le **camoufler** dans un support (texte, image, etc.) de manière à masquer sa présence.

Exemple:


recto

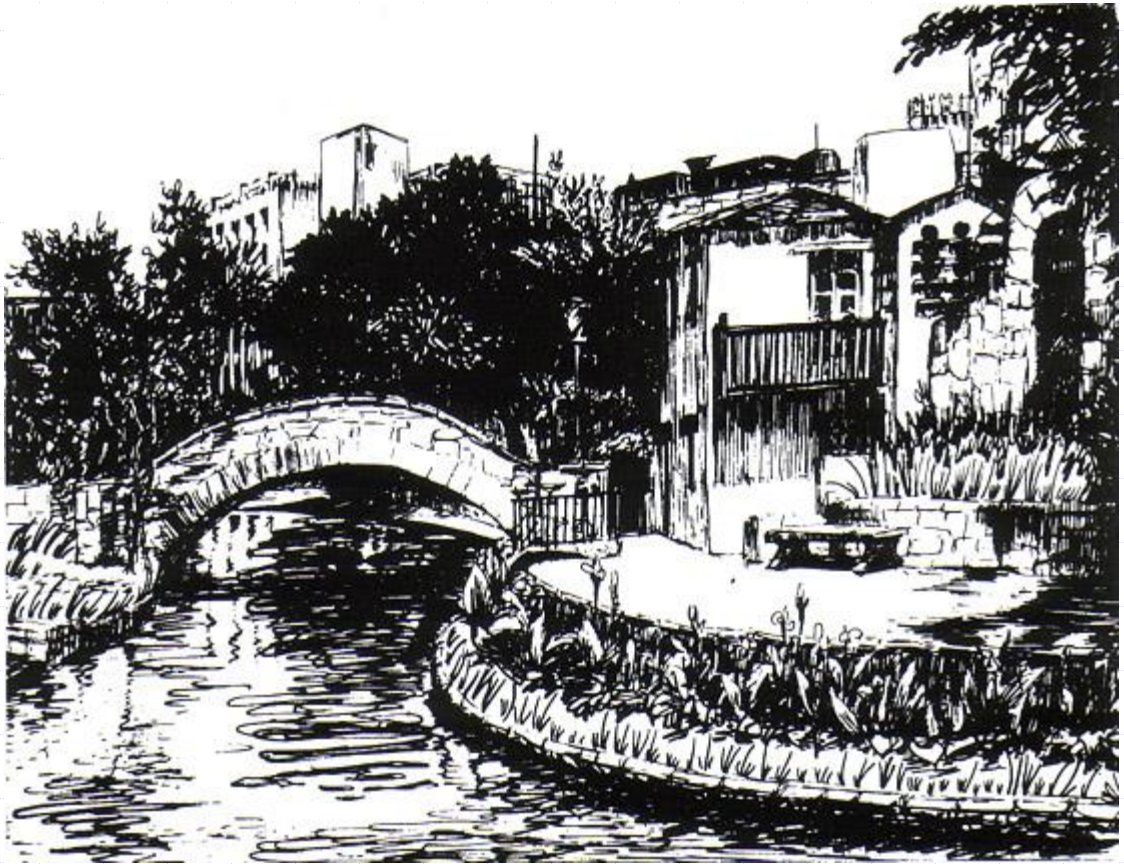

verso

L'image ci-contre a été obtenue en agrandissant fortement le petit carré entouré d'un cercle vert: on a scanné cette partie du billet avec une résolution de 2400 ppi pour voir apparaître le texte (une simple loupe ne permet pas de lire les caractères).

# Définitions des termes courants de cryptologie

## Exemple:

les brins d'herbe le long de la rivière et sur le mur du jardin représentent les traits et les points de l'alphabet Morse



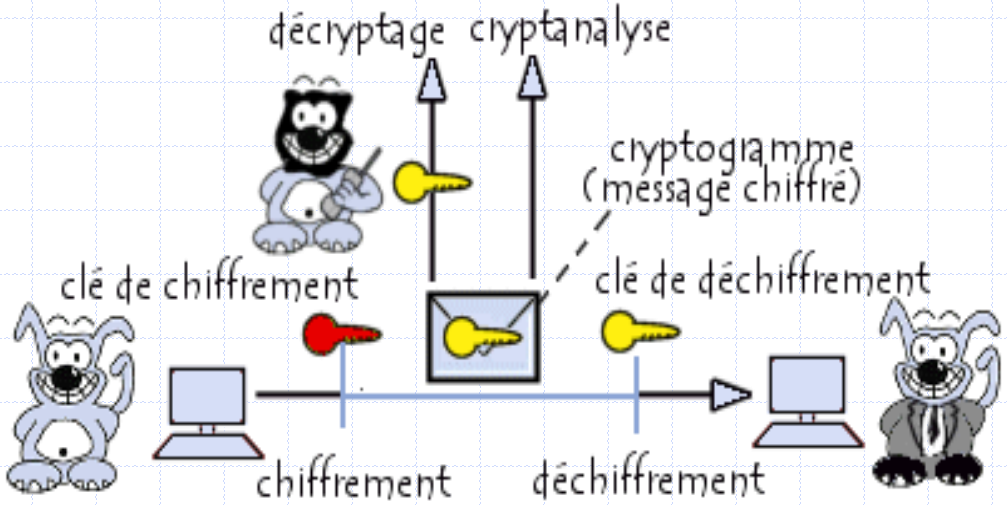
Message caché: Compliments of CPSA MA to our chief Col. Harold R. Shaw on his visit to San Antonio May 11th 1945.

# Plan du cours

1. Terminologie
2. Définition et Historique
3. Service e la cryptographie
4. Cryptographie Classique
5. Cryptographie Moderne
6. Signature électronique
7. Certificat
8. Mises en oeuvre concrètes
9. Cryptanalyse

# Définitions

Le mot **cryptographie** est un terme générique désignant l'ensemble des techniques permettant de **chiffrer** des messages, c'est-à-dire permettant de les rendre inintelligibles sans une action spécifique.




**Fait**

La cryptologie n'est pas la sécurité, mais il n'y a pas de sécurité sans cryptologie

# Exemples historiques de protocoles de cryptographie

1. La scytale
2. Le cryptogramme de César
3. La permutation de lettres
4. Le chiffrement de Vigenère

# Exemples historiques de protocoles de cryptographie

## Scytale


**Message crypté**

KTMIOILMDLONKRIIRGNOHGWT

# Exemples historiques de protocoles de cryptographie

## Cryptogramme de César

$$
\begin{array}{lllllll}
A \to E & B \to F & C \to G & D \to H & E \to I & F \to J & G \to K \\
H \to L & I \to M & J \to N & K \to O & L \to P & M \to Q & N \to R \\
O \to S & P \to T & Q \to U & R \to V & S \to W & T \to X & U \to Y \\
V \to Z & W \to A & X \to B & Y \to C & Z \to D &
\end{array}
$$

**Exemple**

ATTAQUE AU MATIN ⟶ EXXEUYI EY QEXMR

**Clé** : entier entre 1 et 26

# Exemples historiques de protocoles de cryptographie

## Permutations de lettres

$$
\begin{array}{lllllll}
A \to D & B \to R & C \to K & D \to X & E \to V & F \to H & G \to L \\
H \to N & I \to S & J \to O & K \to P & L \to Q & M \to W & N \to I \\
O \to T & P \to J & Q \to E & R \to U & S \to Z & T \to A & U \to C \\
V \to F & W \to B & X \to Y & Y \to G & Z \to M &  &
\end{array}
$$

**Exemple**

ATTAQUE AU MATIN ⟶ DAADECV DC WDASI

**Clé** : permutations sur 26 lettres

**Nombre de clés** : $26! = 403291461126605635584000000 \simeq 2^{88}$

# Exemples historiques de protocoles de cryptographie

## Chiffrement de Vigenère

**Correspondance lettre $\leftrightarrow$ nombre.** $A = 0,\ B = 1,\ \ldots,\ Z = 25$

**Addition sur les lettres.** J + W = F $(9 + 22 \mod 26 = 5)$

**Exemple**

```
NOUS ATTAQUERONS AU MATIN PAR LE NORD
VIGE NEREVIGENER EV IGENE REV IG ENER
KYCY PZMGNEMXDTL GR WIZXT IGO VM TDXW
```

**Clé** : mot de $l$ lettres ($l$ fixé)

**Nombre de clés** : $26^l$ (Note : $26^{19} \simeq 26!$)

# Plan du cours

1. Terminologie
2. Définition et Historique
3. Service e la cryptographie
4. Cryptographie Classique
5. Cryptographie Moderne
6. Signature électronique
7. Certificat
8. Mises en oeuvre concrètes
9. Cryptanalyse

## LA CRYPTO, POURQUOI FAIRE ?

Assurer plusieurs services de sécurité :

- Confidentialité: personne ne doit pouvoir lire les données
- Authenticité: personne ne doit pouvoir contrefaire l'origine des données
- Intégrité: personne ne doit pouvoir modifier les données

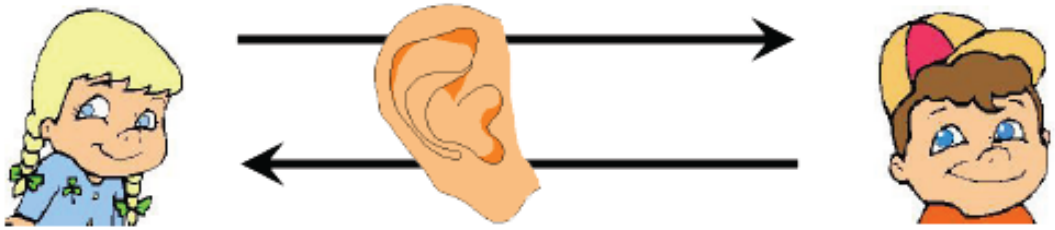
**Fait**

La cryptologie n'est pas la sécurité, mais il n'y a pas de sécurité sans cryptologie.

# LA CONFIDENTIALITE

## S'assurer du caractère secret de l'information

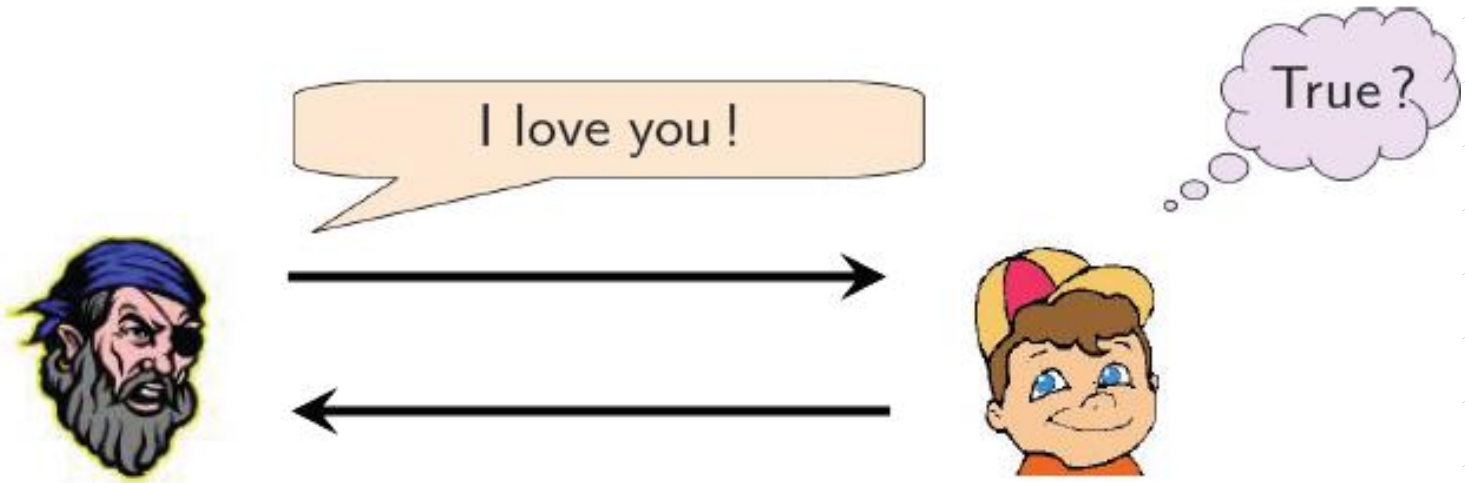
- Échange de messages en présence d'un espion



- Stockage de données sécurise

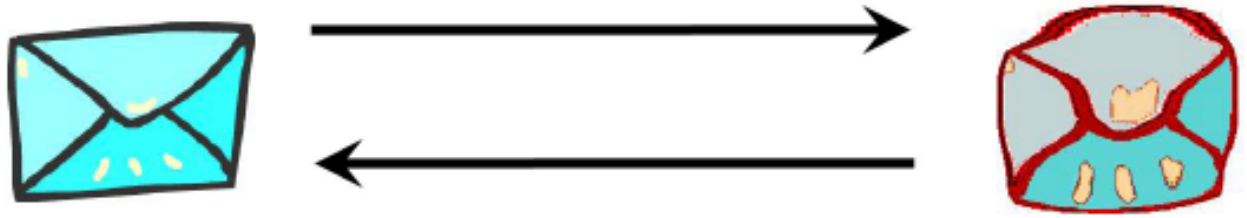
# L'AUTHENTICITE

S'assurer de la provenance d'un message et de l'authenticité de son émetteur



# L'INTEGRITE

## S'assurer de la non modification d'un message



Le contenu de l'enveloppe arrive-t-il < intact > ?

# Plan du cours

1. Terminologie
2. Définition et Historique
3. Service e la cryptographie
4. Cryptographie Classique
   - 4.1 Chiffrement par substitution
   - 4.2 Chiffrement par transposition

# Cryptographie Classique

## Le chiffrement par substitution

Le chiffrement par substitution consiste à remplacer dans un message une ou plusieurs entités (généralement des lettres) par une ou plusieurs autres entités.

**Danger**

Sécurité **faible** : la cryptanalyse par analyse de fréquence révèle immédiatement le type de chiffrement

On distingue généralement plusieurs types de cryptosystèmes par substitution :

# Le chiffrement par substitution

## La cryptographie par substitution monoalphabétique

Le codage par substitution mono-alphabétique est le plus simple à imaginer. Dans le message clair on remplace chaque lettre par une lettre différente.

Exemple: Nous opérons la substitution suivante:

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

Le texte que nous souhaitons coder est le suivant :

UN PETIT ROSEAU M'A SUFFI POUR FAIRE FREMIR L'HERBE

Le texte codé est alors:

MT JCGLG UZVCNM S'N VMWWL JZMU WNLUC WUCSLU Q'DCUYC

# Le chiffrement par substitution

## La cryptographie par substitution monoalphabétique

Pour la première lettre, il y a 26 choix possibles, pour la seconde, 25 choix, etc.... Il existe donc 26! façons de coder distinctes. C'est un nombre en soi assez impressionnant (de l'ordre de 4×1026).

**Obstacle:**

Un des problèmes avec le code par substitution est de se souvenir de la clé (c'est-à-dire la permutation) employée. Il n'est en effet pas facile de se souvenir de 26 lettres dans un ordre **abscon**.

Sécurité

Une recherche exhaustive de la clé est-elle possible ?

26! possibilités de permutations des lettres, soit environ $2^{88}$

$\Longrightarrow$ hors de portée

# La cryptographie par substitution monoalphabétique

C'est pourquoi il existe des variantes :

- Le **chiffre de César**, fondé sur un simple décalage de lettres**.**
- Le **chiffre AtBash.** Il consiste simplement à écrire l'alphabet en sens contraire**.**
- Une variante de la substitution mono-alphabétique : **le carré de Polybe**.

# Le chiffrement par substitution

## La cryptographie par substitution polyalphabétique

Le principe consiste à remplacer chaque lettre du message en clair par une nouvelle lettre prise dans ou plusieurs alphabets aléatoires associés. Par exemple, on pourra utiliser n substitutions mono alphabétiques ; celle qui est utilisée dépend de la position du caractère à chiffrer dans le texte en clair. On choisit une clé qui sert d'entrée dans la grille poly alphabétique incluant autant de symboles qu'il y a de lettres différentes à chiffrer.

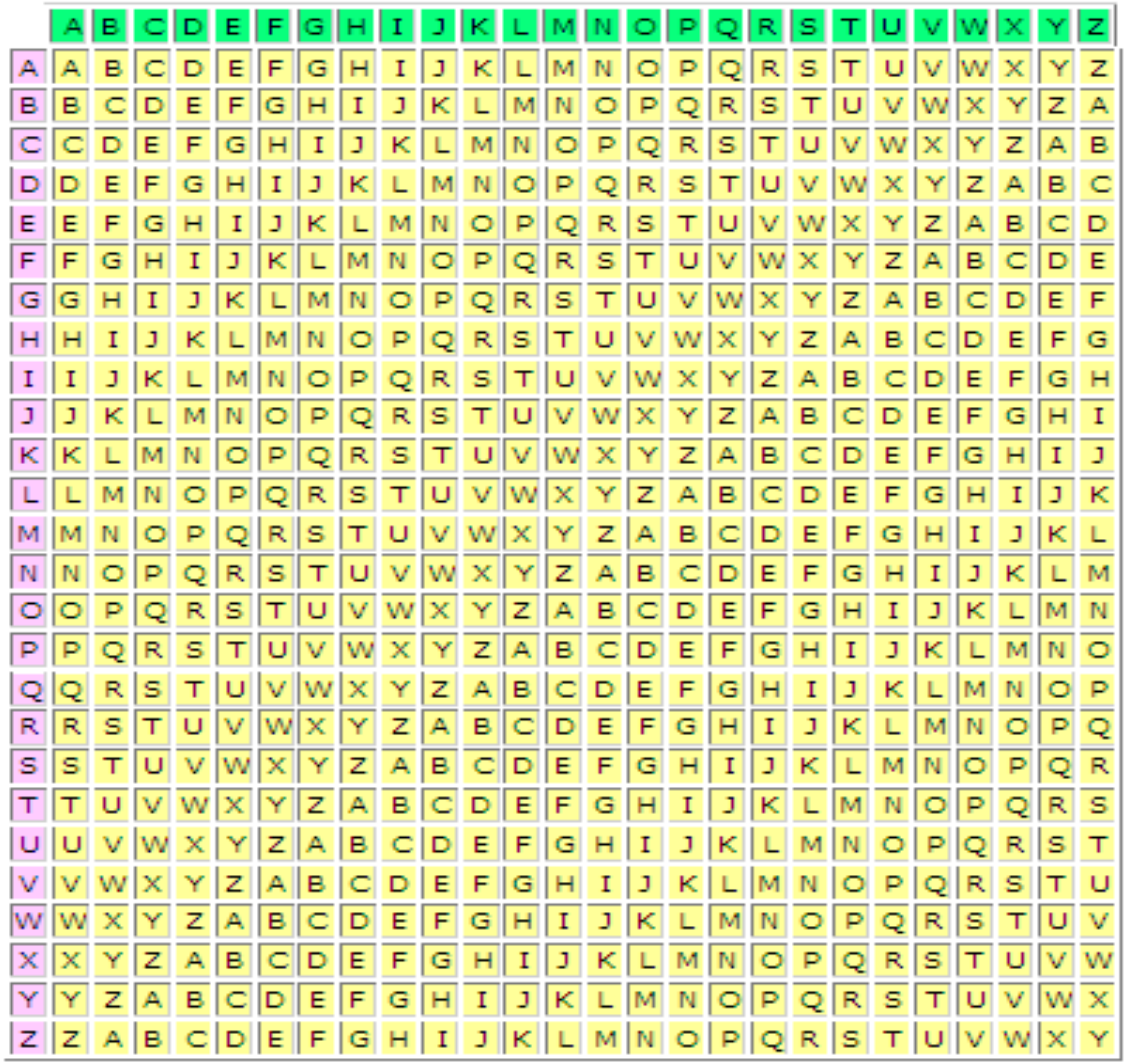
Exemple: Le chiffre de Vigenère

L'idée de Vigenère est d'utiliser un **chiffre de César**, mais où le décalage utilisé change de lettres en lettres. Pour cela, on utilise une table composée de 26 alphabets, écrits dans l'ordre, mais décalés de ligne en ligne d'un caractère. On écrit encore en haut un alphabet complet, pour la clé, et à gauche, verticalement, un dernier alphabet, pour le texte à coder.

# Le chiffrement par substitution

## La cryptographie par substitution polyalphabétique

Pour coder un message, on choisit une clé qui sera un mot de longueur arbitraire.



| | 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 |

# Le chiffrement par substitution

## La cryptographie par substitution polyalphabétique

**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 |

Pour coder la lettre C, la clé est donnée par la lettre M. On regarde dans le tableau l'intersection de la ligne donnée par le C, et de la colonne donnée par le M.

| | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O |
| B | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P |
| C | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q |
| D | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R |
| E | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S |
| F | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T |
| G | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U |

On trouve O. Puis on continue. On trouve :
**ORRWPSHDAIOEI EQ VBNARFDE.**

# Le chiffrement par substitution

## La cryptographie par substitution homophonique

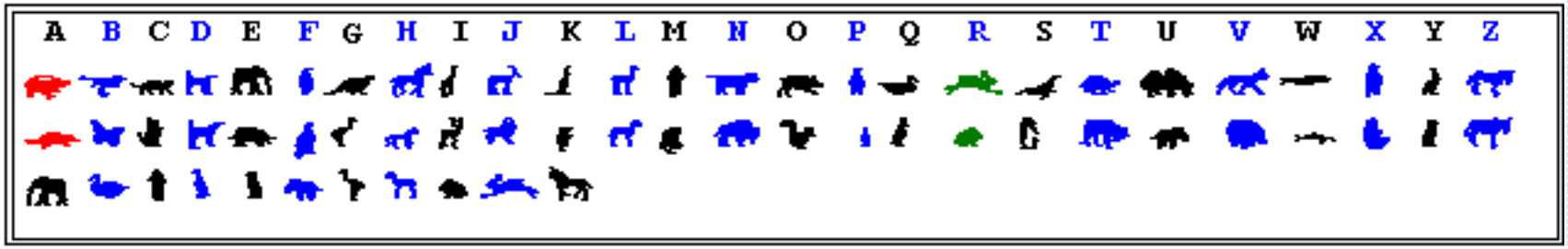
Comme pour le principe précédent, sauf qu'à un caractère du texte en clair on fait correspondre plusieurs caractères dans le texte chiffré.

Ensemble de procédés et ensemble de symboles (lettres, nombres, signes, etc.) employés pour remplacer les **lettres** du message à chiffrer.

Exemple:

*Exemple* : texte en clair = « CHANGEONS LES MENTALITES FRANCAISES »

texte chiffré = «  »




dictionnaire de substitution homophonique

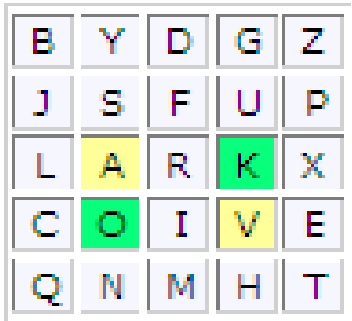
# Le chiffrement par substitution

## La cryptographie par substitution polygrammes

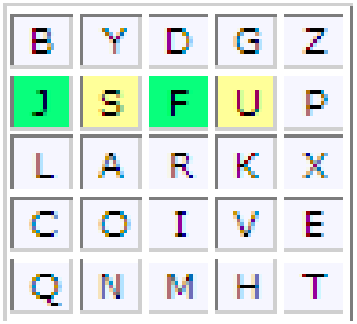
Les caractères du texte en clair sont chiffrés par blocs. Par exemple, " ABA " peut être chiffré par " RTQ " tandis que " ABB " est chiffré par " SLL ". Les exemples les plus célèbres sont les algorithmes de PLAYFAIR et de HILL .

**Exemple:** Le chiffre Playfair

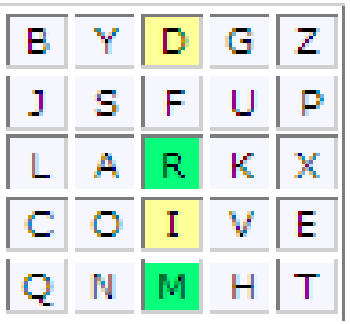
On dispose les 25 lettres de l'alphabet (W exclu car inutile, on utilise V à la place) dans une grille 5x5, ce qui donne la clef. La variante anglaise consiste à garder le W et à fusionner I et J.



Règle 1



Règle 2



Règle 3

# Le chiffrement par substitution

## La cryptographie par substitution polygrammes

**Méthode de chiffrement**

On chiffre le texte par groupes de deux lettres (des **bigrammes**) en appliquant les règles suivantes:

1. Si les deux lettres sont sur les coins d'un rectangle, alors les lettres chiffrées sont sur les deux autres coins. Exemple **OK** devient **VA**, **BI** devient **DC**, **GO** devient **YV**. La première des deux lettres chiffrées est sur la même ligne que la première lettre claire.
2. Si deux lettres sont sur la même ligne, on prend les deux lettres qui les suivent immédiatement à leur droite: **FJ** sera remplacé par **US**, **VE** par **EC**.
3. Si deux lettres sont sur la même colonne, on prend les deux lettres qui les suivent immédiatement en dessous: **BJ** sera remplacé par **JL**, **RM** par **ID**.
4. Si le bigramme est composé de deux fois la même lettre, on insère une nulle (usuellement le X) entre les deux pour éliminer ce doublon.

# Le chiffrement par substitution

## La cryptographie par substitution polygrammes

Pour déchiffrer, on applique les règles ci-dessus à l'envers.

Pour former les grilles de chiffrement, on utilise un **mot-clef secret** pour créer un alphabet désordonné avec lequel on remplissait la grille ligne par ligne.

Exemple:


Message clair : CHIFFREDEPLAYFAIR


Mot-clef : BYDGZJSFUPLARKXCOIVEQNMHT


Message chiffré : VQMRR IIZTX ARDSR OLD

# Cryptage par transposition

Les méthodes de chiffrement par transposition consistent **à réarranger les données à chiffrer de façon à les rendre incompréhensibles**. Il s'agit par exemple de réordonner géométriquement les données pour les rendre visuellement inexploitables. Avec le principe de la transposition **toutes les lettres du message sont présentes, mais dans un ordre différent.** Il utilise le principe mathématique des **permutations**.

Bien entendu, lorsque le nombre de lettres croît, le nombre d'arrangements augmente rapidement et il devient quasiment impossible de retrouver le texte original sans connaître le procédé de brouillage.

# Cryptage par transposition


## Exemple:

Les 27 lettres du message ci-contre, peuvent être disposées de :

**27! = 10'888'869'450'418'352'160'768'000'000 manières.**

Plusieurs types différents de transpositions existent :

# Cryptage par transposition

## Transposition simple par colonnes :

On écrit le message horizontalement dans une matrice prédéfinie, et on trouve le texte à chiffrer en lisant la grille verticalement. Le destinataire légal pour décrypter le message réalise le procédé inverse

Exemple:

*Exemple* : texte à chiffer = « I LOVE MY ENGLISH TEACHER »
utilise une matrice [6;4].

| | | | |
|---|---|---|---|
| I | L | O | V |
| E | M | Y | E |
| N | G | L | I |
| S | H | T | E |
| A | C | H | E |
| R | | | |

texte chiffré = « IENSA RLMGH COYLT HVEIE E »

# Cryptage par transposition

## Transposition complexe par colonnes :

Un mot clé secret (avec uniquement des caractères différents) est utilisé pour dériver une séquence de chiffres commençant à 1 et finissant au nombre de lettres composant le mot clé. Cette séquence est obtenue en numérotant les lettres du mot clé en partant de la gauche vers la droite et en donnant l'ordre d'apparition dans l'alphabet.

On chiffre en écrivant d'abord le message par lignes dans un rectangle, puis on lit le texte par colonnes en suivant l'ordre déterminé par la séquence.

Exemple : texte en clair = «I LOVE MY ENGLISH TEACHER »
utilise le mot clé **SERGIO.**

Clé :

| S | E | R | G | I | O |
|---|---|---|---|---|---|
| 6 | 1 | 5 | 2 | 3 | 4 |

| | | | | | |
|---|---|---|---|---|---|
| I | L | O | V | E | M |
| Y | E | N | G | L | I |
| S | H | T | E | A | C |
| H | E | R | | | |

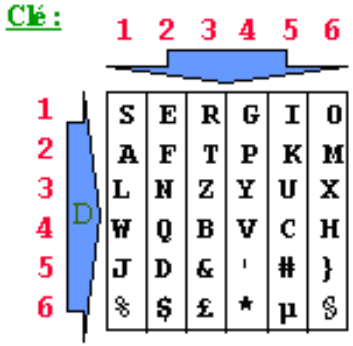
texte chiffré = « LEHEV GEELA MICON TRIYS H »

# Cryptage par transposition

## Transposition par carré polybique :

Un mot clé secret est utilisé pour construire un alphabet dans un tableau. Les coordonnées des lignes et des colonnes correspondant aux lettres du texte à chiffrer sont utilisées pour transcrire le message en chiffres.

Exemple : texte en clair = «CRYPTOLOGY IS A PASSIONATE TOPIC »
utilise le mot clé : **SERGIO.**




texte en clair (coordonnées) : «41322131131122211113212121 4»
« 534436164451242115623236455»

texte fractionné groupé par 2 et recombiné en coordonnées :

«41322131131122211111321212145344361644512421156232364 55»
« G T E R L S F E S S T A A W U V £ % V I Q E J M T £ ' 5»

**texte chiffré avec divisions des mots :**

« GTERL SFESS TAAWU V£%VI QEJMT £'5 »

# Plan du cours

1. Terminologie
2. Définition et Historique
3. Service e la cryptographie
4. Cryptographie Classique
5. Cryptographie Moderne
   - 5.1 Chiffrement à clé secrète
   - 5.2 Chiffrement à clé publique

# La cryptographie moderne

Depuis la Seconde Guerre Mondiale, les besoins cryptographiques ont explosé. Les applications civiles du chiffrement (banques, télécommunications, informatique, cartes bleues...) deviennent un moteur fondamental de progrès. Dans le même temps, un nouveau type de cryptographie est inventé, qui va apporter une sécurité théorique bien supérieure.

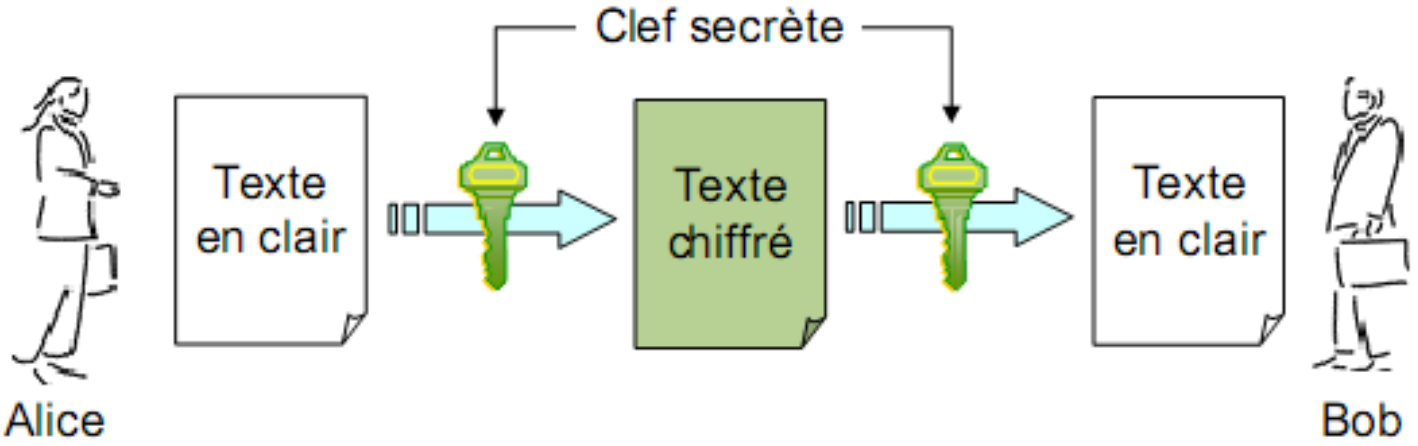
On voit aussi apparaître les deux personnages récurrents les plus célèbres de la cryptographie: **Alice** et **Bob**

Nous vous présentons les cryptosystèmes théoriques, et leurs applications pratiques principales.

# La cryptographie moderne

## Le chiffrement symétrique (chiffrement à clé secrète)

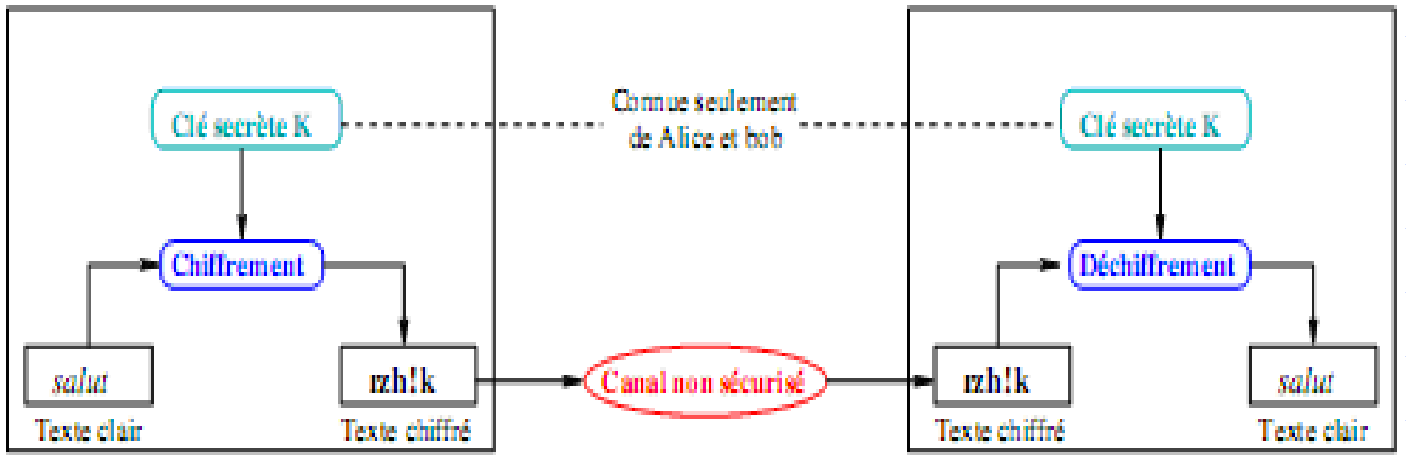
Une même clé est utilisé pour le chiffrement et le déchiffrement, d'ou l'obligation que celle-ci reste confidentielle, sous peine de rendre le système inefficient.




Il y a deux catégories de systèmes à clé privée : les chiffrements par blocs et les chiffrements de flux.

# Le chiffrement symétrique (chiffrement à clé secrète)

## Propriétés




1. **Cle** : La clé de cryptage et la clé de décryptage sont les mêmes et donc doivent être garde es secrètes.
2. **Transformation** : Transformations similaires pour codage et décodage (protocoles symétriques).
3. **Avantage** : Algorithmes en général très rapides
4. **Inconvénient** : Il faut pouvoir échanger la clé !

# Le chiffrement symétrique (chiffrement à clé secrète)

## Le chiffrement par blocs

L'idée générale du chiffrement par blocs est la suivante:

1. Remplacer les caractères par un code binaire (par exemple le code ASCII en base 2). On obtient ainsi une longue chaîne de 0 et de 1.
2. Découper cette chaîne en blocs de longueur donnée, par exemple 64 bits.
3. Chiffrer un bloc en l'additionnant" bit par bit à une clef.
4. Déplacer certains bits du bloc.
5. Recommencer éventuellement un certain nombre de fois l'opération 3. On appelle cela une **ronde**
6. Passer au bloc suivant et retourner au point 3 jusqu'à ce que tout le message soit chiffré.

# Le chiffrement symétrique (chiffrement à clé secrète)

## DES (Data Encryption Standard )

- C'est un chiffrement qui transforme des blocs de **64 bits** avec une clé secrète de 56 bits au moyen de permutations et de substitutions. Le DES est considéré comme étant raisonnablement sécuritaire.

- La clé est en fait constituée de 64 bits, dont 56 bits sont générés aléatoirement et utilisés dans l'algorithme. Les huit autres bits peuvent être utilisés pour la détection d'erreurs. Chacun des huit bits est utilisé comme bit de parité des sept groupes de 8 bits.

- Il utilise les transformations de substitution et de transposition.

- Il y a donc pour le DES $2^{56}$ clés possibles, soit environ ... 72 millions de milliards possibilités.

# DES (Data Encryption Standard )

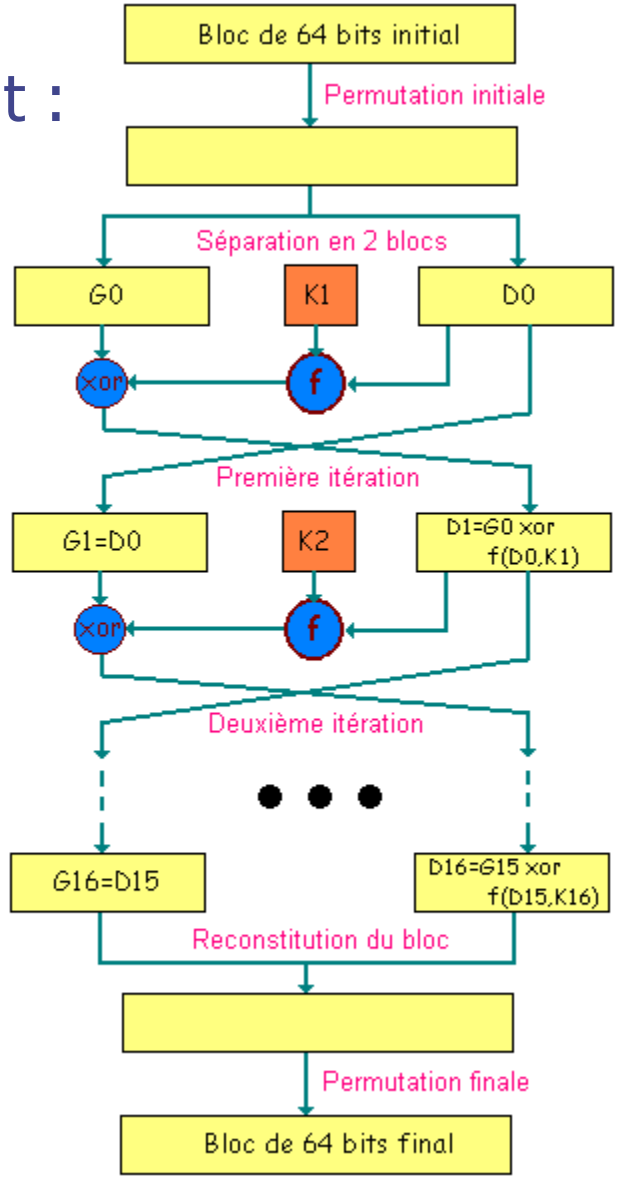
## Les grandes lignes de l'algorithme sont :

- **Phase 1 : Préparation - Diversification de la clé.**
  Le texte est découpé en blocs de 64 bits. On diversifie aussi la clé K, c'est-à-dire qu'on fabrique à partir de K 16 sous-clés $K_1,...,K_{16}$ à 48 bits. Les $K_i$ sont composés de 48 bits de K, pris dans un certain ordre.

- **Phase 2 : Permutation initiale.**
  Pour chaque bloc de 64 bits x du texte, on calcule une permutation finie y=P(x). y est représenté sous la forme $y=G_0D_0$, $G_0$ étant les 32 bits à gauche de y, $D_0$ les 32 bits à droite.

- **Phase 3 : Itération**
  On applique 16 rondes d'une même fonction. A partir de $G_{i-1}D_{i-1}$ (pour i de 1 à 16), on calcule $G_iD_i$ en posant :
  - $G_i=D_{i-1}$.
  - $D_{i-1}=G_{i-1}$ XOR $f(D_{i-1},K_i)$.

- **Phase 4 : Permutation finale.**
  On applique à $G_{16}D_{16}$ l'inverse de la permutation initiale. $Z=P^{-1}(G_{16}D_{16})$ est le bloc de 64 bits chiffré à partir de x



# Le chiffrement symétrique (chiffrement à clé secrète)

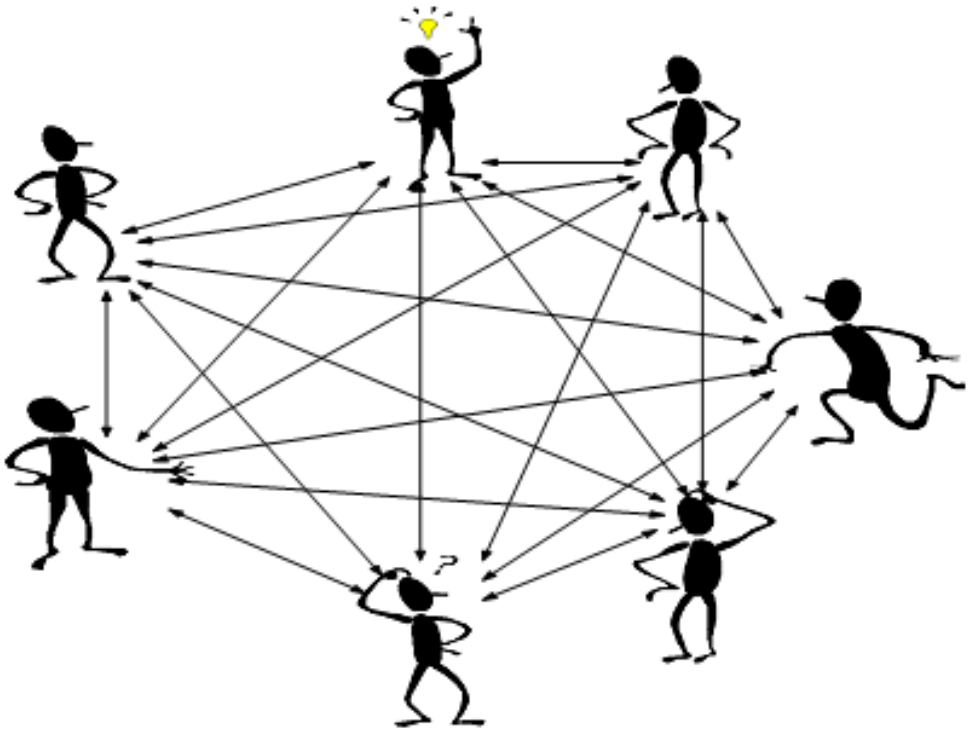
## Chiffrements de flux

Les algorithmes de chiffrement de flux (stream ciphers) peuvent être définis comme étant des algorithmes de chiffrement par blocs, où le bloc a une dimension unitaire (1 bit, 1 octet, etc.) ou relativement petite.

Leurs avantages principaux viennent du fait que la transformation (méthode de chiffrement) peut être changée à chaque symbole du texte clair et du fait qu'ils soient extrêmement rapides.

De plus, ils sont utiles dans un environnement où les erreurs sont fréquentes car ils ont l'avantage de ne pas propager les erreurs (diffusion).

# LES LIMITES DE LA CRYPTOGRAPHIE SYMÉTRIQUE

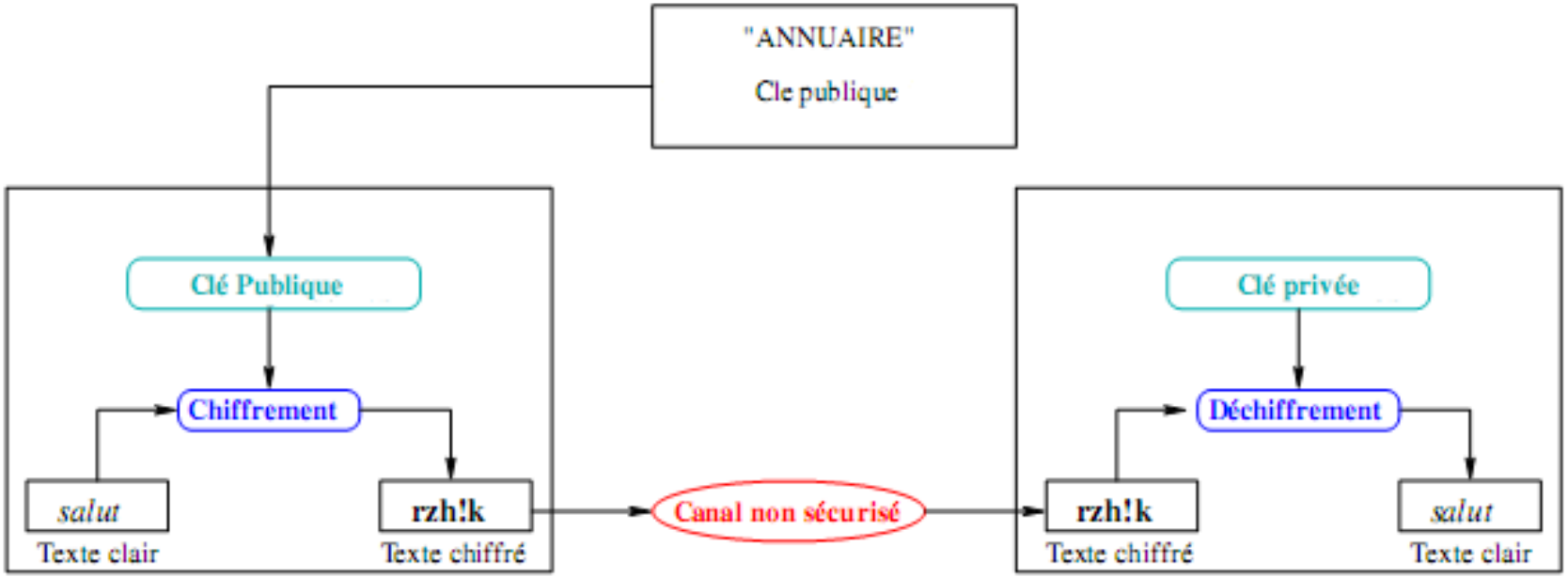


# La cryptographie moderne

## Le chiffrement asymétrique (chiffrement à clé publique)

Dans un cryptosystème asymétrique (ou cryptosystème à clés publiques), les clés existent par paires (le terme de bi-clés est généralement employé) :

- Une clé publique pour le chiffrement ;
- Une clé secrète pour le déchiffrement.



## Le chiffrement asymétrique (chiffrement à clé publique)

- La clé publique est généralement publiée dans un répertoire.

- L'avantage est donc qu'Alice peut envoyer un message à Bob sans communication privée préalable (elle choisit sa clé privée, et la clé publique de Bob). Bob est la seule personne à pouvoir déchiffrer le message en appliquant sa clé secrète et personnelle, et la clé publique d'Alice.

- On dit généralement que chaque clé déverrouille le code produit par l'autre. Une remarque intéressante à faire est qu'avec ce système, même Alice qui a chiffré un message pour Bob, ne pourra déchiffrer le message ainsi codé.

# Caractéristiques du chiffrement asymétrique)

## Avantages

La clé privée ne quitte pas son propriétaire:

- gestion des secrets facilitée
- pas de secret à transmettre

## Inconvénients

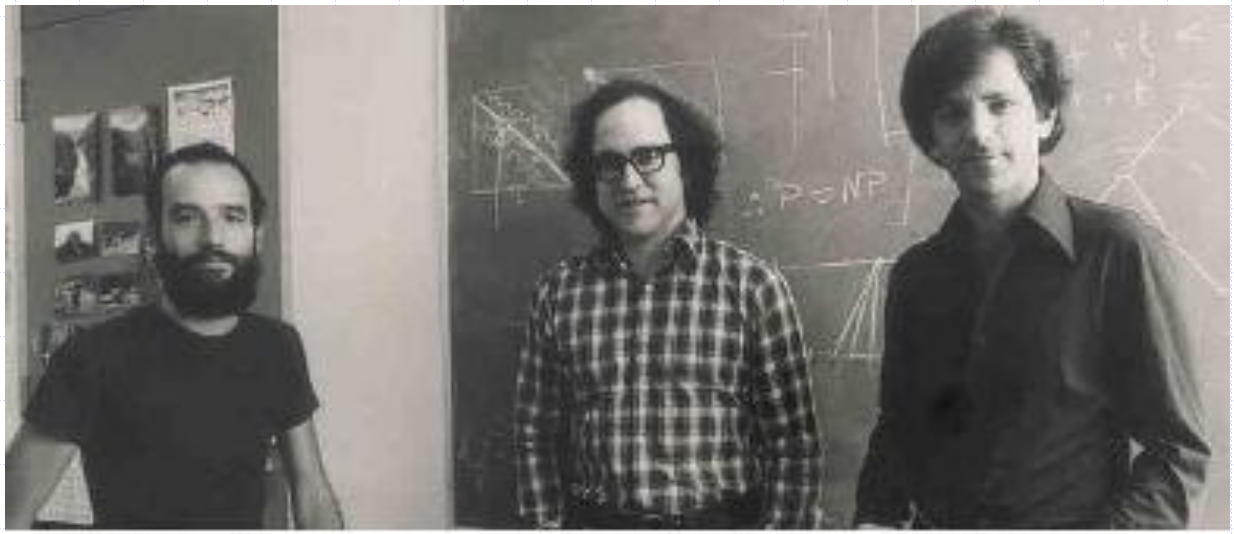
La relation clé publique/clé privée impose:

- des clés plus longues (1024 à 4096 bits)
- des cryptosystèmes beaucoup plus lents qu'en symétrique
- gestion de certificats de clés publiques

# Le chiffrement asymétrique (chiffrement à clé publique)

## Méthode RSA

La méthode de cryptographie RSA a été inventée en 1977 par Ron Rivest, Adi Shamir et Len Adleman, à la suite de la découverte de la cryptographie à clé publique par Diffie et Hellman.




Adi Shamir Ron Rivest Len Adleman

# Méthode RSA

## Principe de fonctionnement du cryptosystème RSA :

Si Bob souhaite recevoir des messages en utilisant le RSA, il procède de la façon suivante :

1. **Création des clés :** Bob crée 4 nombres p,q, e et d :

p et q sont deux grands nombres premiers distincts. Leur génération se fait au hasard, en utilisant un algorithme de test de primalité probabiliste.

e est un entier premier avec le produit (p-1)(q-1).

d est tel que e d=1 modulo (p-1)(q-1). Autrement dit, ed-1 est un multiple de (p-1)(q-1). On peut fabriquer d à partir de e, p et q, en utilisant l'algorithme d'Euclide.

2. **Distribution des clés :** Le couple (n,e) constitue la clé publique de Bob. Il la rend disponible par exemple en la mettant dans un annuaire. Le couple (n,d) constitue sa clé privée. Il la garde secrète.

# Principe de fonctionnement du cryptosystème RSA :

**3. Envoi du message codé :** Alice veut envoyer un message codé à Bob. Elle le représente sous la forme d'un ou plusieurs entiers M compris entre 0 et n-1. Alice possède la clé publique (n,e) de Bob. Elle calcule C=Me mod n. C'est ce dernier nombre qu'elle envoie à Bob.

**4. Réception du message codé** : Bob reçoit C, et il calcule grâce à sa clé privée D=Cd (mod n). D'après un théorème du mathématicien Euler, D=Mde=M (mod n). Il a donc reconstitué le message initial.

# Méthode RSA

## Intérêt de la méthode

Tout l'intérêt du système RSA repose sur le fait qu'à l'heure actuelle il est pratiquement impossible de retrouver dans un temps raisonnable **p** et **q** à partir de **n** si celui-ci est très grand .

**Alice** est donc la seule à pouvoir calculer **d** dans un temps court. De plus, elle n'a jamais à transmettre les entiers **p** et **q**, ce qui empêche leur piratage.

Exemple:

**n**=5141=53·97 et **e**=7, premier avec 52·96=4992).
Il transforme en nombres son message en remplaçant par exemple chaque lettre par son rang dans l'alphabet.

"JEVOUSAIME" devient : "10 05 22 15 21 19 01 09 13 05".

# Méthode RSA

## Exemple (suite):

Puis il découpe son message chiffré en blocs de même longueur représentant chacun un nombre plus petit que **n**

Son message devient : **"010 052 215 211 901 091 305"**

Un bloc **B** est chiffré par la formule $\mathbf{C = B^e \bmod n}$, où **C** est un bloc du message chiffré que **Bob** enverra à **Alice**

Après avoir chiffré chaque bloc, le message chiffré s'écrit : **"0755 1324 2823 3550 3763 2237 2052".**

## Déchiffrement

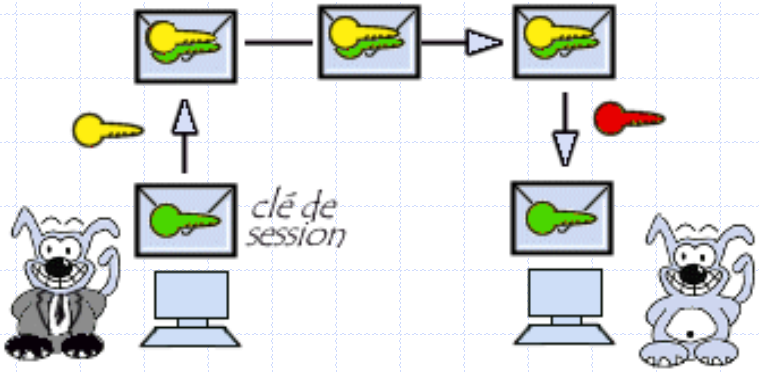
**Alice** calcule à partir de **p** et **q**, **qu'elle a gardés secrets**, la clef **d** de déchiffrage (c'est sa **clef privée**). Celle-ci doit satisfaire l'équation $\mathbf{e \cdot d \bmod ((p-1)(q-1)) = 1}$. Ici, **d**=4279.

Chacun des blocs **C** du message chiffré sera déchiffré par la formule $\mathbf{B = C^d \bmod n}$

Elle retrouve : **"010 052 215 211 901 091 305"**

# Clefs de session

Le principe de la clé de session est simple : il consiste à générer aléatoirement une clé de session de taille raisonnable, et de chiffrer celle-ci à l'aide d'un algorithme de chiffrement à clef publique (plus exactement à l'aide de la clé publique du destinataire).




Le destinataire est en mesure de déchiffrer la clé de session à l'aide de sa clé privée. Ainsi, expéditeur et destinataires sont en possession d'une clé commune dont ils sont seuls connaisseurs. Il leur est alors possible de s'envoyer des documents chiffrés à l'aide d'un algorithme de chiffrement symétrique.

# Algorithme de Diffie-Hellman (1)

L'algorithme de Diffie-Hellman (du nom de ses inventeurs Diffie et Hellman) a été mis au point en 1976 afin de permettre l'échange de clés à travers un canal non sécurisé

Alice et Bob se sont mis d'accord sur un algorithme à clé secrète à utiliser, ils veulent s'échanger une **clé K,** mais ils ne disposent pas de canal fiable pour cela. Diffie et Hellman suggèrent l'échange suivant :

- Alice et Bob choisissent, ensemble et publiquement, un nombre premier p, et un entier $1< a< p$.
- Alice choisit secrètement x1, et Bob choisit secrètement x2.
- Alice envoie à Bob $a^{x1}$, et Bob calcule $K=(a^{x1})^{x2}=a^{x1x2}$ [p].
- Bob envoie à Alice $a^{x2}$, et Alice calcule $K=(a^{x2})^{x1}=a^{x1x2}$ [p].

Alice et Bob sont donc en possession d'une même clé secrète K, qu'ils ne se sont pas échangés directement .

# Algorithme de Diffie-Hellman (2)

Si quelqu'un a espionné leurs conversations, il a en sa possession :

$p, a, a^{x1}$ et $a^{x2}$.

Pour obtenir K, il doit pouvoir calculer x1, en connaissant a,p et $a^{x1}$.

Autrement dit, il doit pouvoir résoudre l'équation (en x) $y=ax\ [p]$.

On appelle ceci résoudre le logarithme discret. Quand les valeurs de p, a et x sont très grandes, il s'agit d'un problème très difficile.

# Plan du cours

1. Terminologie
2. Définition et Historique
3. Service e la cryptographie
4. Cryptographie Classique
5. Cryptographie Moderne
6. Signature électronique
7. Certificat
8. Mises en oeuvre concrètes
9. Cryptanalyse

# Signature électronique

## Signature : Idée générale

Reproduire les caractéristiques d'une signature manuscrite

1. Lier un document à son auteur
2. Rendre la signature difficilement imitable
3. Responsabilité de l'auteur (juridique. . .)

# Signature électronique

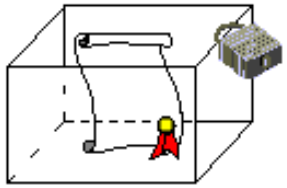

Le paradigme de **signature électronique** (appelé aussi signature numérique) est un procédé permettant de garantir l'authenticité de l'expéditeur (fonction d'authentification) et de vérifier l'intégrité du message reçu.

La signature électronique assure également une fonction de non-répudiation, c'est-à-dire qu'elle permet d'assurer que l'expéditeur a bien envoyé le message

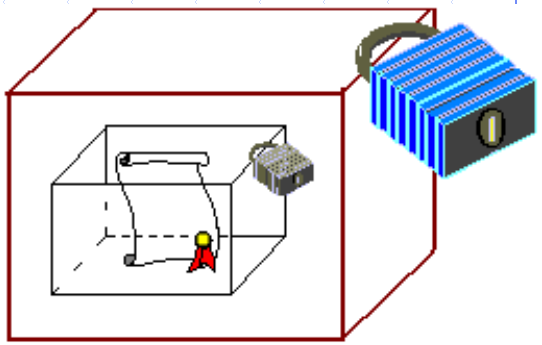
Exemple: Alice veut donc envoyer un message crypté à Bob, mais Bob veut s'assurer que ce message provient bien d'Alice. Ils se sont mis d'accord sur un système de cryptographie à clé publique commun,

# Signature électronique

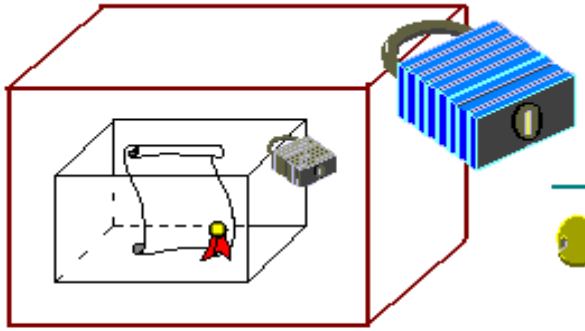
## Exemple (suite) :



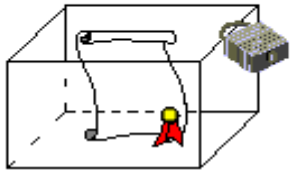
enferme le message dans une boite à l'aide de sa clé privée (authentification de l'expéditeur)



enferme cette boite dans une autre boite avec la clé publique de Bob (chiffrement, seul Bob peut ouvrir)



recoit le message chiffré et authentifié



ouvre la premičre botie avec sa clé privée (déchiffrement)

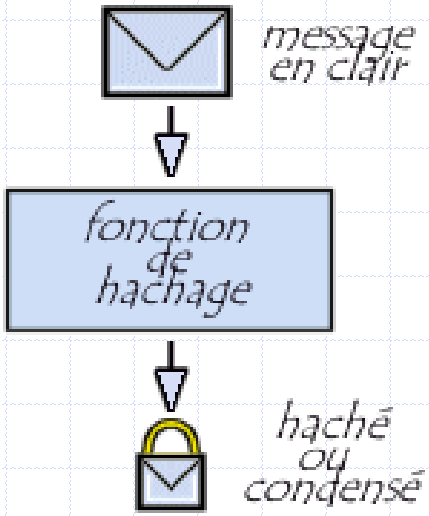
ouvre la deuxičme boite avec la clé publique d'Alice (authentification)

# Signature électronique

## Fonctions de hachage ?

Habituellement, pour réduire la taille des messages, **une fonction de hachage** est utilisée pour créer une empreinte du message et c'est cette empreinte que l'on chiffre.

Une fonction de hachage calcule le résumé d'un texte. Ce résumé doit être à sens unique, pour éviter de reconstituer le message initial connaissant seulement le résumé.




Il doit être très sensible, c'est-à-dire qu'une petite modification du message entraîne une grande modification du résumé.

# Signature électronique

## Fonctions de hachage ?

Cette fonction (H), qui doit être rapide à calculer, transforme un message M de longueur arbitraire en une **empreinte numérique** h de **taille fixée**:

**h = H(M), où h est de longueur m.**

Cette fonction doit en outre avoir les propriétés suivantes:

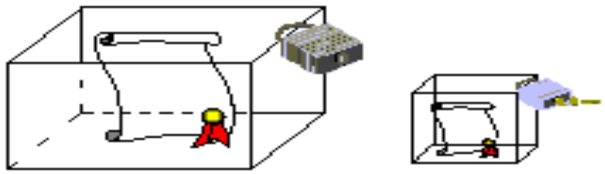
- étant donné un message M, il est facile de calculer l'empreinte h,
- étant donné une empreinte h, il est difficile de calculer le message M,
- résistance forte à la collision: il est difficile de trouver deux messages M et M' tels que H(M)=H(M').

# Signature électronique

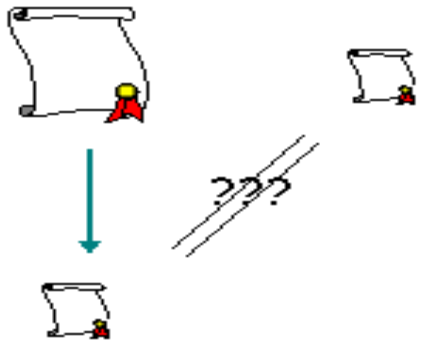
## Fonctions de hachage ? Vérification d'intégrité

la fonction de hachage, couplée à la cryptographie à clé publique, permet d'authentifier l'expéditeur

Calcule le résumé du message



Met le message dans une boite que seul Bob peut ouvrir.
Met le résumé dans une boite que elle seule peut fermer.




Ouvre les 2 boites.
Calcule le résumé du message recu.
Le compare avec le résumé envoyé.
S'ils sont égaux, le message a été envoyé correctement, et il est sûr que c'est Alice l'expéditeur.

# Signature électronique

## Fonctions de hachage ?

Les algorithmes de hachage les plus utilisés actuellement sont :

- **MD5** (MD signifiant Message Digest). Développé par Rivest en 1991, MD5 crée une empreinte digitale de 128 bits à partir d'un texte de taille arbitraire en le traitant par blocs de 512 bits. Il est courant de voir des documents en téléchargement sur Internet accompagnés d'un fichier MD5, il s'agit du condensé du document permettant de vérifier l'intégrité de ce dernier)

- **SHA** (pour Secure Hash Algorithm, pouvant être traduit par Algorithme de hachage sécurisé) crée des empreintes d'une longueur de 160 bits SHA-1 est une version améliorée de SHA datant de 1994 et produisant une empreinte de 160 bits en le traitant par blocs de 512 bits.

L' algorithme MD5 se déroule en plusieurs étapes.

**Etape 1 : Complétion**

Le message est constitué de b bits m1...mb. On complète le message par un 1, et suffisamment de 0 pour que le message étendu ait une longueur congruente à 448, modulo 512. Puis on ajoute à ce message la valeur de b, codée en binaire sur 64 bits. On obtient donc un message dont la longueur totale est un multiple de 512 bits. On va travailler itérativement sur chacun des blocs de 512 bits.

**Etape 2 : Initialisation**

On définit 4 buffers de 32 bits A,B,C et D, initialisés ainsi (les chiffres sont hexadécimaux, ie a=10, b=11...).

A=01234567
B=89abcdef
C=fedcba98
D=76543210

On définit aussi 4 fonctions F,G,H et I, qui prennent des arguments codés sur 32 bits, et renvoie une valeur sur 32 bits, les opérations se faisant bit à bit.

F(X,Y,Z) = (X AND Y) OR (not(X) AND Z)
G(X,Y,Z) = (X AND Z) OR (Y AND not(Z))
H(X,Y,Z) = X xor Y xor Z
I(X,Y,Z) = Y xor (X OR not(Z))

Ce qu'il y a d'important avec ces 4 fonctions et que si les bits de leurs arguments X,Y et Z sont indépendants, les bits du résultat le sont aussi.

**Etape 3 : Calcul itératif**

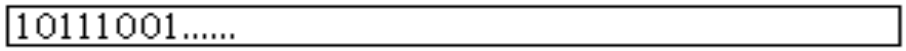
Pour chaque bloc de 512 bits du texte, on fait les opérations suivantes :

on sauvegarde les valeurs des registres dans AA,BB,CC,DD.
on calcule de nouvelles valeurs pour A,B,C,D à partir de leurs anciennes valeurs, à partir des bits du bloc qu'on étudie, et à partir des 4 fonctions F,G,H,I.
on fait A=AA+A, B=BB+B, C=CC+C, D=DD+D.

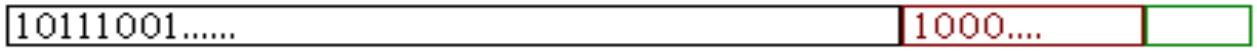
**Etape 4 : Ecriture du résumé**

Le résumé sur 128 bits est obtenu en mettant bout à bout les 4 buffers A,B,C,D de 32 bits.

Message initial



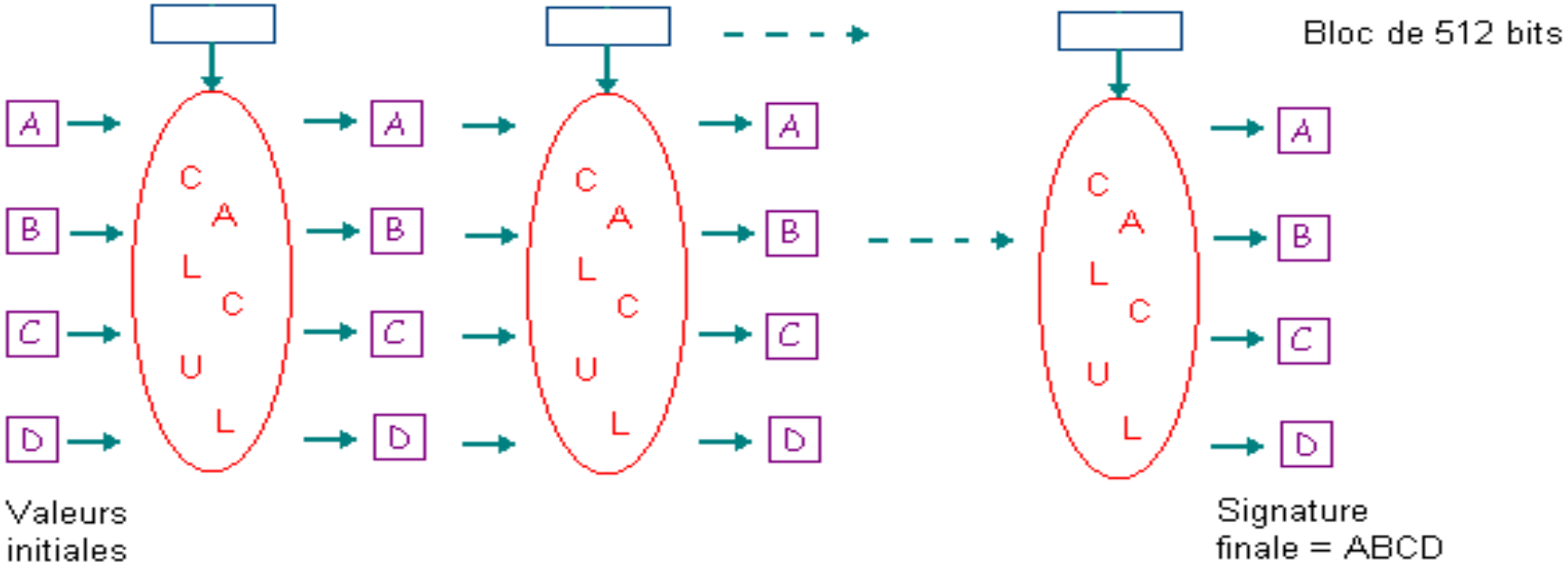

Complétion




Message Complétion Longueur

Découpage en blocs de 512 bits

Calcul de la signature




**Description du fonctionnement du MD5**

# Plan du cours

1. Terminologie
2. Définition et Historique
3. Service e la cryptographie
4. Cryptographie Classique
5. Cryptographie Moderne
6. Signature électronique
7. Certificat
8. Mises en oeuvre concrètes
9. Cryptanalyse

# Certificat

Le problème des certificats numériques est à l'opposé de celui de la signature électronique .

Cette fois, c'est donc du Destinataire que l'on veut être sûr, et non de l'Expéditeur.

- Ainsi un certificat permet d'associer une clé publique à une entité (une personne, une machine, ...) afin d'en assurer la validité.
- Le certificat est en quelque sorte la carte d'identité de la clé publique, délivré par un organisme appelé autorité de certification

# Certificat [Principe]

## Exemple:

Comme dans la vie courante, on a recours à des certificats. Pour passer un examen, il vous faut prouver votre identité, ie fournir une carte d'identité, passeport ou permis de conduire. Un organisme supérieur (l'Etat) a signé ces certificats, s'assurant auparavant (par un acte de naissance,...) qu'il s'agit bien de vous.

Les certificats numériques fonctionnent sur le même principe

Alice veut certifier que sa clé publique lui appartient.

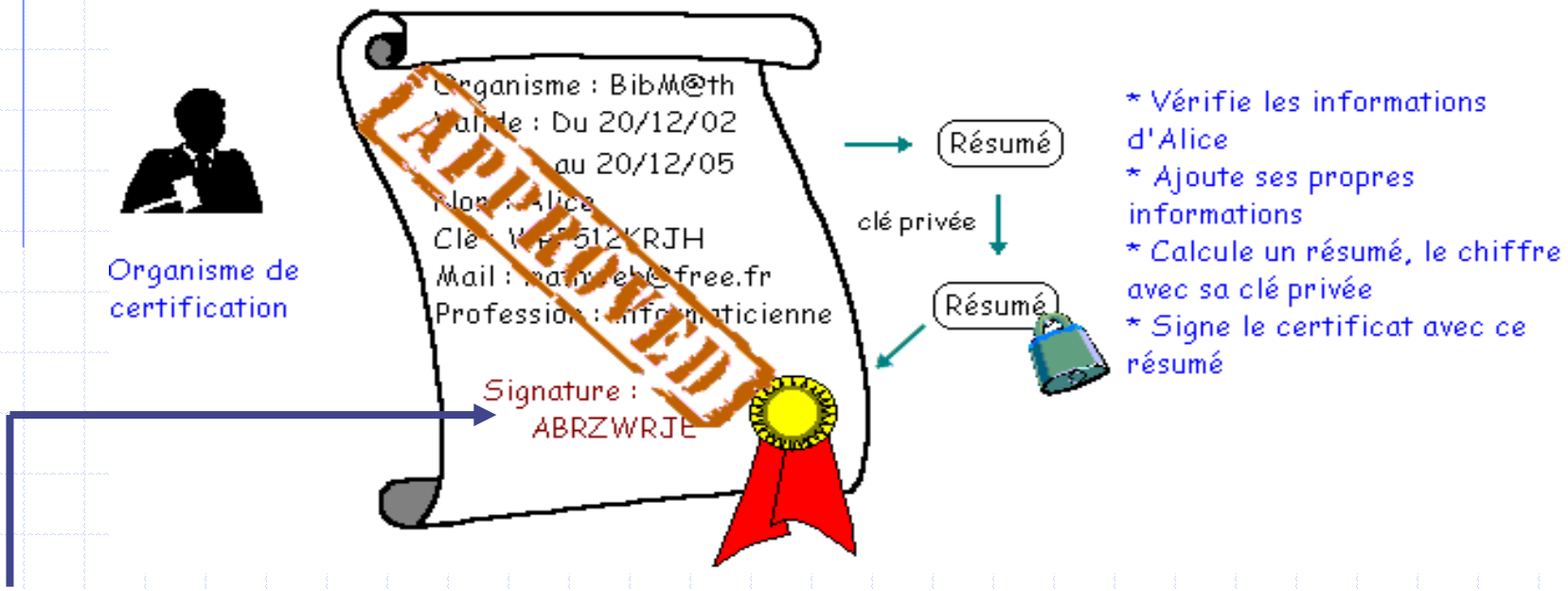
Alice

Nom : Alice
Clé : WRP512KRJH
Mail : mathweb@free.fr
Profession : informaticienne

Alice fournit une fiche d'identité à l'organisme de certification.

# Certificat [Principe]

- Cet organisme vérifie les informations fournies par Alice, et ajoute au certificat son propre nom, une date limite de validité, et surtout une signature numérique.

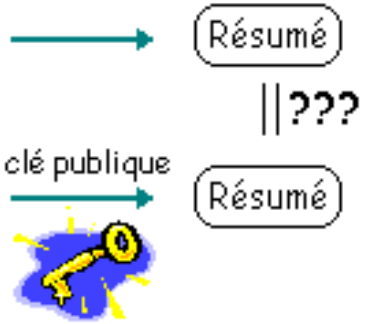



Cette signature est calculée de la façon suivante : A partir des informations du certificat, l'organisme calcule un résumé en appliquant une fonction de hachage connue. Puis il signe ce résumé en lui appliquant sa clé secrète.

# Certificat [Principe]

Lorsque Bob veut envoyer son message à Alice, il télécharge le certificat de celle-ci sur un serveur de certificat (on parle de PKI, **Public Key Infrastructure**). Il calcule le résumé du certificat, puis applique la clé publique de l'organisme auteur du certificat à la signature électronique. Si cette quantité est égale au résumé, il est sûr qu'il a bien affaire à Alice.

Bob

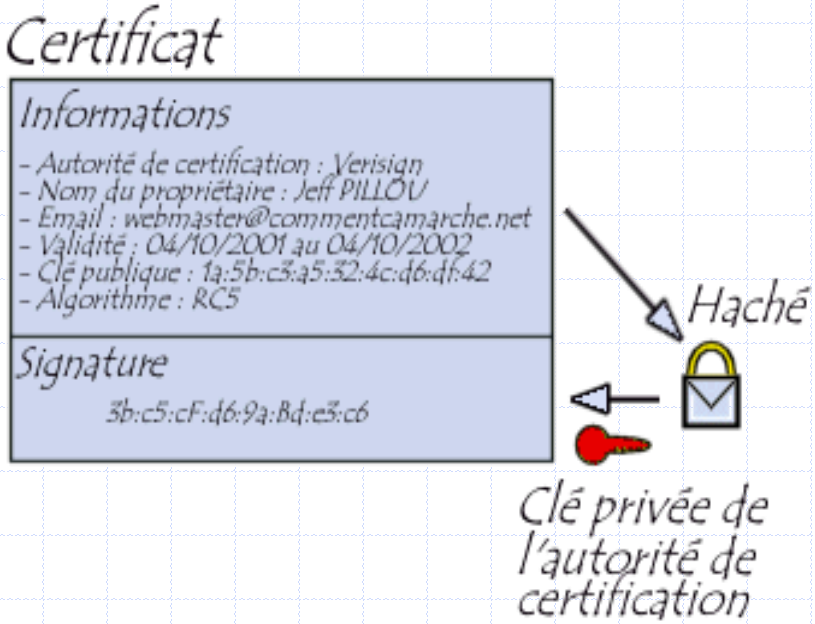




* Télécharge le certificat
* Calcule son résumé
* "Ouvre" la signature avec la clé publique de l'organisme
* Compare les 2 résumés

# Structure d'un certificat

Les certificats sont des petits fichiers divisés en deux parties :

- La partie contenant les informations
- La partie contenant la signature de l'autorité de certification



# Types d'usages

Les certificats servent principalement dans trois types de contextes :

- Le **certificat client**

```
Version: 3 (0x2)
Serial Number:
    5c:e4:85:54:9e:84:f0:59:90:fd:08:7a:62:93:6d:36
Signature Algorithm: md5WithRSAEncryption
Issuer: L=Internet, O=VeriSign, Inc., OU=VeriSign OnSite Admin Demo
Validity
    Not Before: Nov  8 00:00:00 2000 GMT
    Not After : Jan  7 23:59:59 2001 GMT
Subject: O=HSC, OU=www.verisign.com/repository/CPS Incorp. By Ref.,LIAB.LTD(c)96,
    CN=Ghislaine Labouret/Email=ghislaine.labouret@hsc.fr
Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (1024 bit)
        Modulus (1024 bit):
            00:bd:da:6b:f7:7d:6c:4e:cb:00:9f:61:56:4c:7d:
            ...
        Exponent: 65537 (0x10001)
```

```
X509v3 extensions:
    X509v3 Basic Constraints:
        CA:FALSE
    X509v3 Certificate Policies:
        Policy: 2.16.840.1.113733.1.7.1.1
          CPS: https://www.verisign.com/CPS
          User Notice:
            Organization: VeriSign, Inc.
            Number: 1
            Explicit Text: VeriSign's CPS incorp. by reference liab. ltd. (c)97 VeriSign
    Netscape Cert Type:
        SSL Client
    2.16.840.1.113733.1.6.11:
        . 2f5941537bae90da19e157922c4e3992
    2.16.840.1.113733.1.6.13:
      ....
Signature Algorithm: md5WithRSAEncryption
    85:5a:83:d3:4c:a8:f4:59:69:10:f0:4f:f2:94:87:19:ab:cd:
    ...
```

# Types d'usages

Les certificats servent principalement dans trois types de contextes :

- Le **certificat serveur**
- Le **certificat VPN**

```
Version: 3 (0x2)
Serial Number: 20 (0x14)
Signature Algorithm: md5WithRSAEncryption
Issuer: C=FR, ST=Ile-de-France, L=Levallois-Perret, O=Herv\xE9 Schauer Consultants (HSC),
    OU=Certificate Authority, CN=HSC CA/Email=ca@hsc.fr
Validity
  Not Before: Oct 27 07:29:34 2000 GMT
  Not After : Nov 11 07:29:34 2000 GMT
Subject: C=FR, ST=Ile de France, L=Levallois-Perret, O=HSC, OU=IPsec 2000 testbed,
    CN=kame.ipsec2000.fr
Subject Public Key Info:
  Public Key Algorithm: rsaEncryption
  RSA Public Key: (1024 bit)
    Modulus (1024 bit):
      00:f8:51:89:b7:0c:33:56:74:a5:28:98:ed:60:6c:
      ...
    Exponent: 65537 (0x10001)
X509v3 extensions:
  X509v3 Key Usage: critical
    Digital Signature, Non Repudiation
  X509v3 Subject Alternative Name:
    email:kame@ipsec2000.fr, IP Address:192.168.1.60
Signature Algorithm: md5WithRSAEncryption
  3d:77:f0:f9:9f:9c:6a:f7:1a:ee:2c:bd:0f:57:a2:23:93:35:
  ...
```

# Plan du cours

1. Terminologie
2. Définition et Historique
3. Service e la cryptographie
4. Cryptographie Classique
5. Cryptographie Moderne
6. Signature électronique
7. Certificat
8. Mises en oeuvre concrètes
9. Cryptanalyse

# Mises en oeuvre concrètes

## La sécurité des cartes bancaires

Lorsqu'on introduit sa carte bleue dans un distributeur automatique, on imagine assez mal tout ce qui se passe **!!!!!!**

Chacun sait qu'il faut rentrer son code secret pour pouvoir débloquer le paiement, mais ceci n'est que la face cachée de la sécurité des cartes bleues. Comment être sûr que personne ne peut fabriquer de fausse carte, prendre votre identité bancaire, et dépenser votre argent **??????**


- Créée par deux ingénieurs français, à la fin des années 1970.
- La puce est une sorte de petit ordinateur, avec un processeur qui permet d'effectuer des calculs, une mémoire dont une partie est accessible en écriture (enregistrement de l'historique des transactions), une autre en lecture seule, et enfin une dernière en lecture cachée.

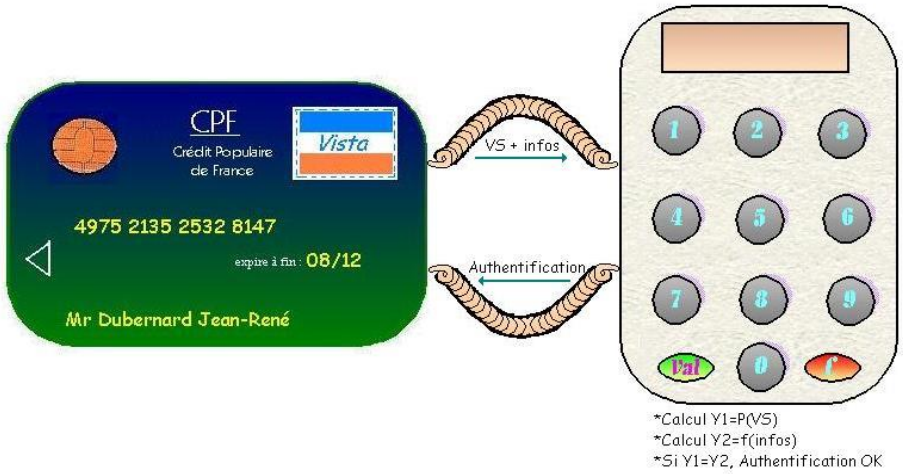
# La sécurité des cartes bancaires

## Mécanisme de paiement par carte bleue

Lorsque l'on introduit sa carte dans le terminal du commerçant, il se déroule un processus en plusieurs étapes :

### 1. Authentification de la carte

Lorsque la carte est introduite dans le terminal, celui lit les informations portées par la carte, et la valeur de signature VS. Il calcule alors Y1=f(info), et Y2=P(VS)=P(S(Y)), P étant la clé publique du GIE. Puis il compare Y1 et Y2 : pour qu'une carte soit valide, il faut que Y1=Y2.



# La sécurité des cartes bancaires

## Mécanisme de paiement par carte bleue

### 2. Code confidentiel

Le code secret est stocké (sous forme chiffrée) à la fois dans la puce et sur la piste magnétique de la carte. Dans la premier cas, c'est la puce de la carte qui elle-même vérifie si le code entré est le bon, et transmet sa réponse au terminal.

### 3. Authentification en ligne (par le DES)


**1.** Le centre envoie à la carte une valeur aléatoire x

**2.** La carte calcule y=f(x,K), où K est une clé secrète, inscrite dans la partie illisible de la carte, et f est la fonction de chiffrement du DES.

**3.** La valeur y est retransmise au centre, qui lui-même calcule f(x,K), et donne ou non l'autorisation

# Plan du cours

1. Terminologie
2. Définition et Historique
3. Service e la cryptographie
4. Cryptographie Classique
5. Cryptographie Moderne
6. Signature électronique
7. Certificat
8. Mises en oeuvre concrètes
9. Cryptanalyse

# Cryptanalyse – Attaques classiques

L'attaquant connaît les algorithmes de cryptage et décryptage.

- **Attaque à texte crypté uniquement** : l'attaquant ne dispose que d'un ou plusieurs messages cryptés qu'il souhaite décrypter. C'est le type d'attaque le plus difficile .

- **Attaque à texte clair connu** : l'attaquant dispose d'exemple s de messages clairs avec les mes sages cryptés correspondants, ou d'une partie clair d'un message crypté. Le but es t alors de trouver la clé.

# Cryptanalyse – Attaques classiques

- **Attaque à texte clair choisi** : l'attaquant peut obtenir la version cryptée d'un certain nombre de messages clairs choisis, soit a priori (attaque hors ligne), soit au fur et à mesure (attaque en ligne ). Le but est encore de trouver la clé.
- **Attaque à texte crypté choisi** : l'attaquant peut obtenir la version cryptée d'un certain nombre de messages clairs choisis, et aussi la version claire d'un certain nombre de messages cryptés choisis. On distingue encore entre attaques hors ligne et en ligne.

# Cryptanalyse – Autre types d'attaques

- **Attaque par le paradoxe des anniversaires** : Il s 'agit d'obtenir des collisions (utilisation deux fois d'une même valeur) pour obtenir de l'information. Si on utilise $2^n$ valeurs possibles, on peut espérer la première collision avec environ $2^{n/2}$ valeurs .

- **Attaque par pré-calcul** : Il s'agit pour l'attaquant de pré-calculer des informations et de s'en servir pour créer des collisions. Cela nécessite plus de travail mais permet aussi plus de fléxibilité. Un cas extrême est la recherche exhaustive .

- **Attaque de différentiation** : Il s 'agit d'une attaque qui permet de différencier le protocole de cryptage utilisé d'un protocole de cryptage parfait. Cela couvre les attaques citées précedemment et toutes les attaques à venir !