# Cryptographie

# Notions de base

Sommaire

# Généralités

- objectifs globaux :

  → garder secret / ne pas communiquer ;

  → rétention d'information ;

  → principe du camouflage, déguisement, porte close, …

- Genèse : utilisée depuis l'antiquité (chiffrement de César) ;
- Origine Arabe : "cypher" vient de zéro "sifr" ( صـفر )
- Au début un art puis devenue une science au XXI$^{e}$ siècle ;
- Utilisation simplifiée grâce à l'outil informatique;

## Pourquoi chiffrer ?

**Confidentialité** : mécanisme pour transmettre des données de telle sorte que seul le destinataire autorisé puisse les lire.

**Intégrité** : mécanisme pour s'assurer que les données reçues n'ont pas été modifiées durant la transmission.

**Authentification** : mécanisme pour permettre d'identifier des personnes ou des entités et de certifier cette identité.

**Non-répudiation** : mécanisme pour 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.

Vocabulaire autour de la cryptographie :

**chiffrement** : transformation, à l'aide d'une clé, d'un message en clair en message chiffré ;

**chiffre** : utilisation de la substitution au niveau des lettres ;

**code** : utilisation de la substitution au niveau des mots ou phrases pour coder ;

**coder** : utilisation d'un code sur un texte ;

**cryptogramme** : message chiffré ;

**cryptosystème** : algorithme de chiffrement ;

Vocabulaire autour de la cryptographie :

**décrypter** : retrouver le message clair à partir du message chiffré sans connaître la clé ;

**cryptanalyse** : science de l'analyse des cryptogrammes pour les décrypter ;

**cryptographie** : étude de l'art du chiffrement ;

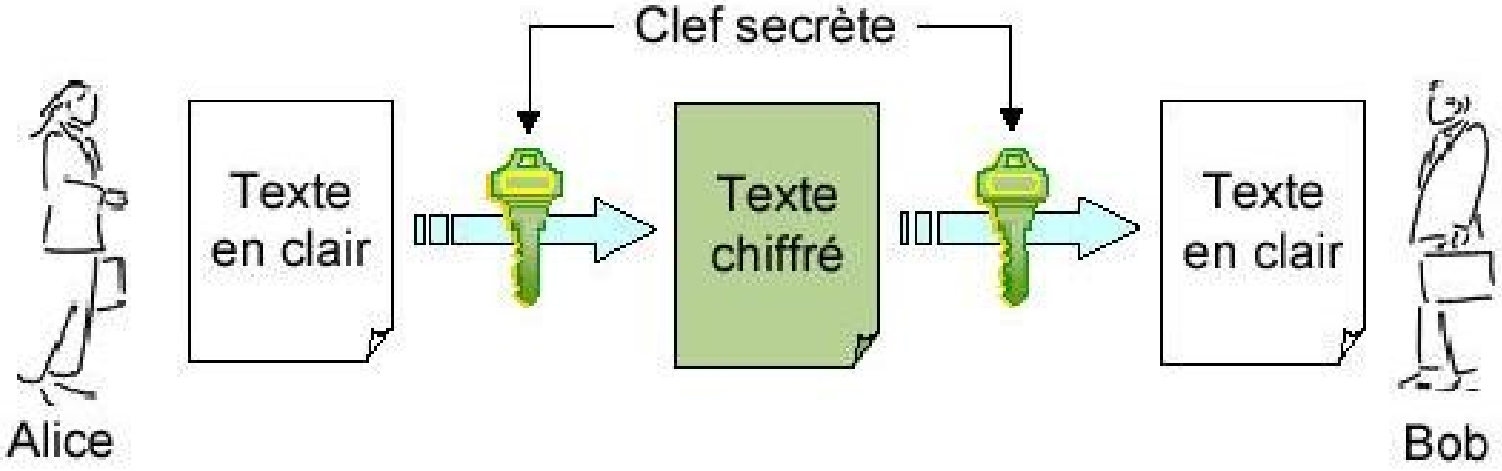
**cryptologie** : science regroupant la cryptanalyse ET la cryptographie ;

**cryptolecte** : vocable utilisé par un groupe d'individus utilisant la cryptographie;

# Principes de fonctionnement

Chiffrement symétrique :

- La même clé est utilisée pour chiffrer ET déchiffrer ;
- Nécessité de garder la clé totalement confidentielle ;
- Mise en œuvre complexe si grand nombre de participants.

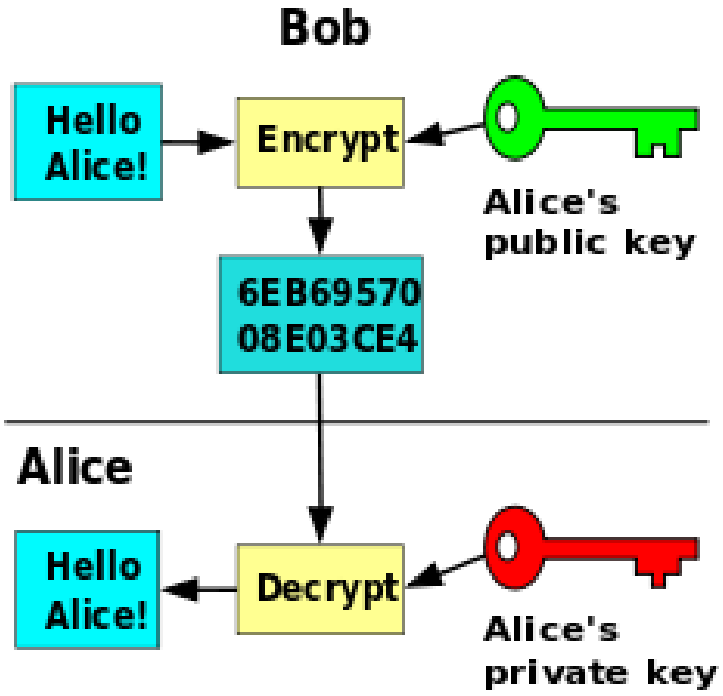


Chiffrement asymétrique :

• Inventé pour résoudre le problème de l'échange des clés ;

• Deux clés :

→ publique pour le chiffrement ;
→ privée pour le déchiffrement.




•La clé publique est mise à disposition de tous (eg. Public Key Server) ;

• Le message ne peut être déchiffré qu'avec la clé privée que le destinataire garde précieusement ;

Fonction de hachage :

• Fonction qui permet de calculer pour un ensemble très grand un résultat précis (eg. chaîne de caractères de taille fixe) ;

• Souvent utilisé pour calculer des empreintes de gros fichiers ;

• Représentation ou empreinte plus simple à manipuler en mémoire que le fichier source ;

• Fonction à sens unique → opération inverse impossible ;

• Est souvent utilisée pour garantir l'intégrité (non modification par une tierce personne).

# Opérations utilisées

Effet d'avalanche :

• propriété très recherchée ;

• provoque des modifications de plus en plus importantes dans le cryptosystème ;

• une modification mineure de l'entrée provoque une modification majeure de la sortie,

• 1/2 est un bon effet d'avalanche (*Strict Avalanche Criterion*)

→ pour 1 bit d'entrée modifié ;

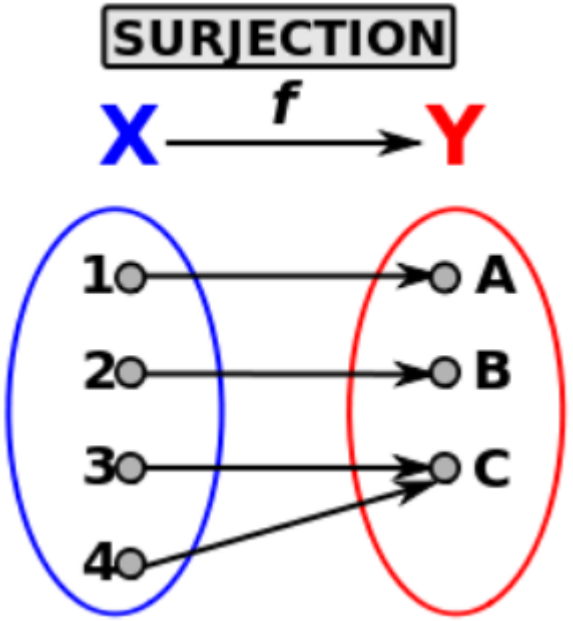
→ 50 % des bits de sortie changent.

## Effet d'avalanche → pourquoi ?

• rend l'inversion plus difficile (retrouver la fonction utilisée dans le cryptosystème) ;

• empêche ou rend très difficile les recherches par biais statistique (indice de coïncidence) ;

• si la primitive de chiffrement a un mauvais effet d'avalanche il est possible de faire des prédictions sur les entrées en observant les sorties.




$$\forall y \in Y,\ \exists x \in X,\ f(x) = y$$

• cryptosystème de hachages

→ utilisation de fonction surjective ;

→ attention aux collisions ;

→ *X* doit être grand.

Permutation :

• P-Box ou « permutation box » désigne une table de permutation utilisée dans les algorithmes de chiffrement ;

• Indique comment échanger les éléments d'une structure ;

• augmente la « diffusion » :

→ mélange des données ;
→ effet d'avalanche.

• Se présente sous la forme d'un tableau à une dimension :

→ exemple pour un octet [ 5, 4, 1, 3, 7, 8, 2, 6 ] ;

| Index | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | Signification |
|---|---|---|---|---|---|---|---|---|---|
| Chiffre | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 146 |
| Code | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 104 |

Substitution :

• S-Box ou « substitution box » désigne une table de substitution utilisée dans les algorithmes de chiffrement ;

• contribue à la « confusion » → rend l'information originale inintelligible ;

• casse la linéarité de la structure de chiffrement ;

• la table de substitution prend en paramètre *x* bits et en renvoie *y* ou $x > y$ ;

Substitution :

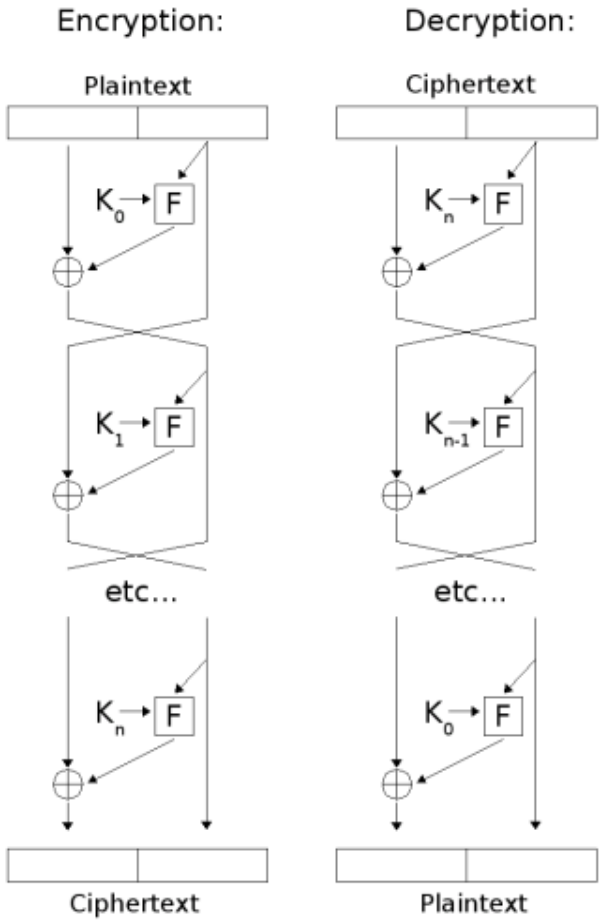
- Prenons la table de substitution suivante

| S-Box | | 3 bits LSB | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | 000 | 001 | 010 | 100 | 011 | 101 | 110 | 111 |
| Bit MSB | 1 | 1000 | 0100 | 1001 | 0111 | 1110 | 0011 | 1101 | 0000 |
| | 0 | 0110 | 1011 | 0010 | 1100 | 0101 | 1111 | 0001 | 1110 |

- Prenons l'entrée suivante : « 0101 0001 1001 1111 »

- Avec la table de substitution cela donne :

| 0101 → 1111 | 0001 → 1011 | 1001 → 0100 | 1111 → 0000 |
|---|---|---|---|
| Le message devient : 1111 1011 0100 0000 | | | |




Réseau de Feistel (Horst Feistel) :

• Utilisé dans les algorithmes de chiffrement par bloc ;

• Première utilisation dans Lucifer et DES ;

• Chiffrement et déchiffrement ont une structure similaire (voire identique) ;

• Principe :

→ on découpe l'information en deux blocs ;
→ un bloc est codé avec une clé ou sous-clé (dérivée) ;
→ le bloc codé est ajouté à l'autre avec un XOR ;
→ on réitère le processus un certain nombre de tours (eg. 16)

Ou exclusif :

• Très utilisé dans les algorithmes de chiffrements symétriques ;

• Propriétés mathématiques intéressantes :

→ $A \oplus A = 0$
→ $A \oplus 0 = A$
→ $A \oplus 1 = \bar{A}$
→ $A \oplus \bar{A} = 1$
→ commutativité
→ associativité

| Table de vérité de XOR | | |
|---|---|---|
| **A** | **B** | **R = A ⊕ B** |
| 0 | 0 | 0 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 0 |

Ou exclusif :

| Table de vérité de XOR | | |
|---|---|---|
| A | B | R = A ⊕ B |
| 0 | 0 | 0 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 0 |

- Considérons un document à chiffrer :

0110 1010 1101 0100

- Considérons la clé suivante : 1010

- On obtient le message codé suivant :

| | | | | |
|---|---|---|---|---|
| message clair | 0110 | 1010 | 1101 | 0100 |
| clé de chiffrement | 1010 | 1010 | 1010 | 1010 |
| message codé | 1100 | 0000 | 0111 | 1110 |

## Ou exclusif :

| Table de vérité de XOR | | |
|---|---|---|
| **A** | **B** | **R = A ⊕ B** |
| 0 | 0 | 0 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 0 |

- On réalise la même opération pour déchiffrer :

| | | | | |
|---|---|---|---|---|
| message codé | 1100 | 0000 | 0111 | 1110 |
| clé de chiffrement | 1010 | 1010 | 1010 | 1010 |
| message clair | 0110 | 1010 | 1101 | 0100 |

- Dans un réseau de Feistel :
  - → on coupe le message en deux
  - → on code la moitié avec la clé
  - → on fait un XOR avec l'autre moitié

# Chiffrements faibles

La scytale lacédémonienne :

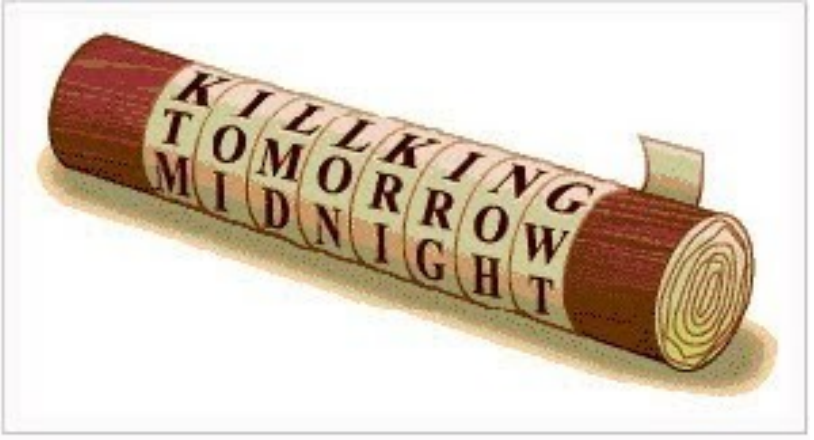
• première trace de procédé de dissimulation intentionnel ;

• bâton que se transmettent les coureurs de courses de relais ;

Principe :
• destinataire et émetteur ont deux bâtons strictement identiques ;
• l'émetteur enroule une courroie autour du bâton ;
• l'émetteur écrit le message puis déroule la courroie ;
• le destinataire n'a qu'à enrouler la courroie autour de son bâton pour lire le message !

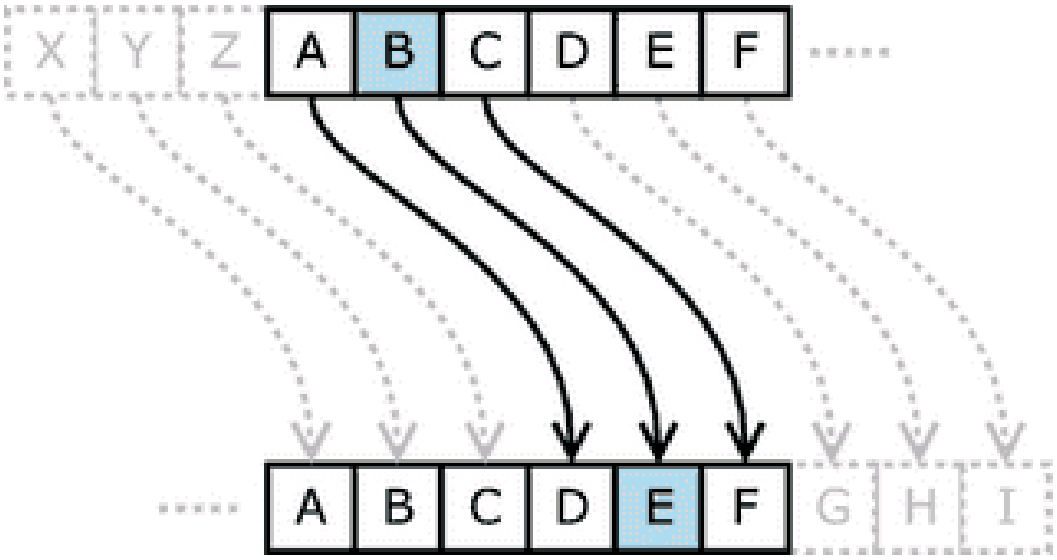
Message chiffré :

KTMIOILMDLONKRIIRGNOHGWT



Le chiffre de César :

- procédé de chiffrement par substitution monoalphabétique ;
- on remplace les lettres par d'autres (décalage de l'alphabet) ;
- présent encore de nos jours sous le nom ROT13 ;
- faiblesse à l'analyse de fréquence.




Le chiffrement de Vigenère :

- procédé de chiffrement par substitution polyalphabétique ;
- on remplace les lettres par d'autres ;
- le remplacement se fait en fonction de la lettre ainsi que de sa position dans le mot ;
- résiste à l'analyse de fréquence.

## Le chiffrement de Vigenère :

- considérons la table de chiffrement suivante :

texte en clair

lettre de la clé

lettre du code

| | 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 de Vigenère :

• Prenons un exemple :

→ codons le message suivant : «la crypto c'est trop bien» ;

→ utilisons la clé suivante : « epsi » ;

→ on répète la clé sous le message à chiffrer puis on utilise la table de permutation :

| | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| l | a | | c | r | y | p | t | o | | c | , | e | s | t | | t | r | o | p | | b | i | e | n |
| e | p | | s | i | e | p | s | i | | e | , | p | s | i | | e | p | s | i | | e | p | s | i |
| p | p | | u | z | c | e | l | m | | g | , | t | k | b | | x | g | g | x | | f | x | w | v |

Stéganographie :

- Pas à proprement parler un procédé cryptologique → cacher et non chiffrer ;

- Utiliser une image ou un texte pour cacher de l'information ;

message transmis par un espion allemand pendant le premier conflit → mondial

Mili tu m infin
i tus eſt exerc itus
ac prope diem ini
bunt be llum, ex plo rato
res omnes deprehen ſi ſu nt,
capite pœn as de dere.

Gratæ Miliſie tuæ fuere literæ, preſertim cum infini ſcrip tus eſt ludus, quo ſe exercet Titus noſter familiaris, ac prope modum in diem inimicus, propterea ama bunt bene illum, ſi is exemplo eorum, rato que modo res omnes deprehendet, at ſi ſumunt, alij rem à ſummo capite, eum pœnitebit illas amplius deri dere.
vale.

Honor Militiæ tuus fuit Carolus pater, nam cum infini to vic tus eſt, cum minima exercitu inuitus parte hoſtis fugit, ac prope vltimum diem iniurius peribit, necabunt Bere illum, atque extem plo puer Arato peribit, res omnes deprehenſæ bonæ ſi ſunt, ante Syllam, & optimo capite non pœnitentias amplius deci dere ſperabit. vale.

# Chiffrement absolu (masque jetable)

Masque jetable :

• Le masque jetable ou chiffre de Vernan est un algorithme de cryptographie ;

• Ce chiffrement impose des conditions particulières pour la clé :

→ elle doit être aussi longue que le message ;
→ les caractères la composant doivent être aléatoires ;
→ chaque clé ne doit être utilisée qu'une seule fois.

• La méthode de combinaison entre le message clair et la clé est suffisamment simple pour être employée « à la main » ;

Masque jetable :

• Si les trois préceptes précédants sont respectés, le système offre une **sécurité théorique absolue** ;

• Explication :

→ si on connaît uniquement le texte chiffré ;
→ que toutes les clés sont équiprobables ;
→ alors tous les textes clairs sont possible ;

• Analyse statistique impossible ;

Masque jetable :

• Connaître une partie du texte clair et chiffré permet de connaître uniquement la partie de la clé :

→ le reste de la clé est différente de la partie connue
→ aucune information supplémentaire ne peut être trouvée !

• On atteint le niveau de sécurité maximal : la sécurité sémantique ;

• On ne cherche plus la complexité du calcul comme avec les autres algorithmes ;

• Le masque jetable est dit **inconditionnellement sûr**.

Masque jetable :

- Prenons le message suivant : « ECOLEEPSI »
- Prenons la clé suivante : « OVERWATCH »
- Attribuons à chaque lettre un rang (A → 0, B → 1, …)
- On additionne les rangs du message et du masque ;
- Si on dépasse le rang maximal ou soustrait le rang maximal au résultat (modulo) → ici modulo 26 ;

## Masque jetable :

- On chiffre le message ainsi :

| message | 4 (E) | 2 (C) | 14 (O) | 11 (L) | 4 (E) | 4 (E) | 15 (P) | 18 (S) | 9 (I) |
|---|---|---|---|---|---|---|---|---|---|
| clé | 14 (O) | 21 (V) | 4 (E) | 17 (R) | 22 (W) | 0 (A) | 19 (T) | 2 (C) | 7 (H) |
| clé + message | 18 | 23 | 18 | 28 | 26 | 4 | 34 | 20 | 16 |
| modulo | 18 | 23 | 18 | 3 | 1 | 4 | 9 | 20 | 16 |
| message chiffré | S | X | S | D | B | E | J | U | Q |

Masque jetable :

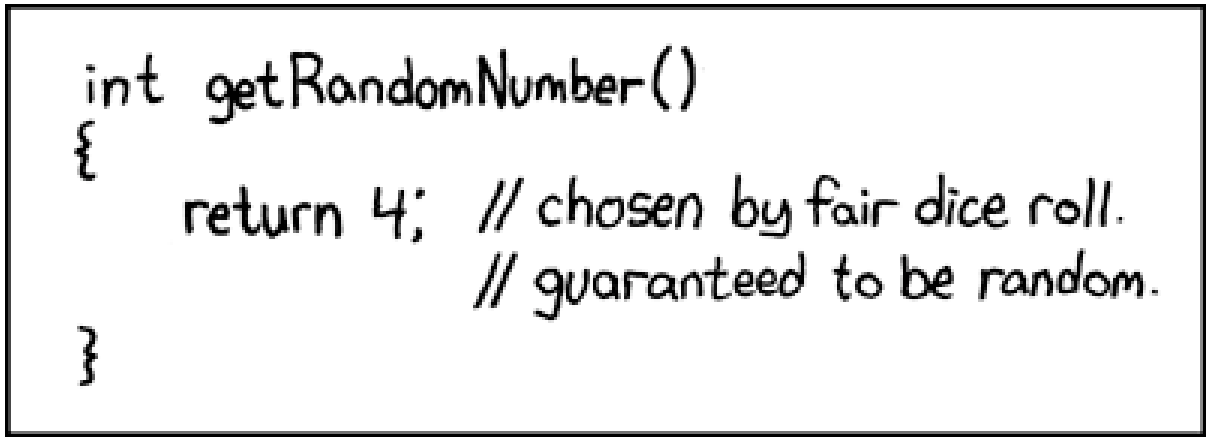
- On déchiffre le message ainsi :

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| message chiffré | 18 (S) | 23 (X) | 18 (S) | 3 (D) | 1 (B) | 4 (E) | 9 (J) | 20 (U) | 16 (Q) |
| clé | 14 (O) | 21 (V) | 4 (E) | 17 (R) | 22 (W) | 0 (A) | 19 (T) | 2 (C) | 7 (H) |
| message - clé | 4 | 2 | 14 | -14 | -21 | 4 | -10 | 18 | 9 |
| modulo | 4 | 2 | 14 | 11 | 4 | 4 | 15 | 18 | 9 |
| message | E | C | O | L | E | E | P | S | I |

Masque jetable :

- Limitations du système :

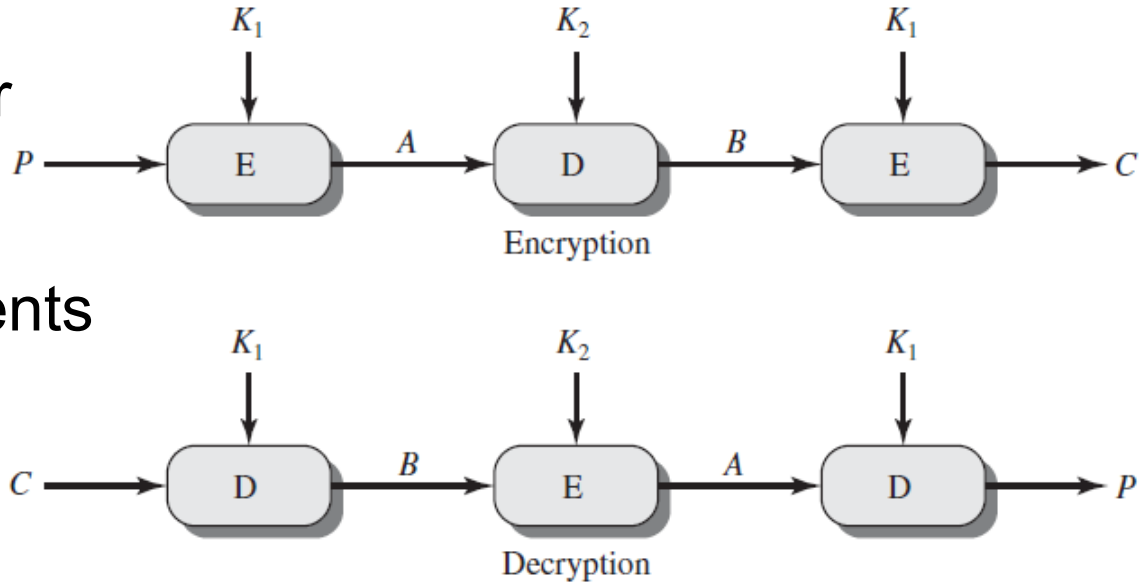
→ taille des clés pour les messages longs ;
→ nombre de clés ;
→ transmission des clés ;
→ comment générer des clés vraiment aléatoires ?



# Chiffrements symétriques

3DES :

• Algorithme de chiffrement par bloc ;




• Enchaînement de 3 chiffrements DES sur le même bloc ;

• Bloc de 64 bits ;

• Utilisation de 2 ou 3 clés différentes ;

• Utilisation EDE compatible avec le DES (encypt, decrypt, encrypt) si on utilise 3 fois la même clé ;

• Quand :

→ K1 = K3 alors la clé fait 112 bits de long

→ K1!= K3 alors la clé fait 168 bits de long

3DES :

- Formule du mode de Tuchman :

$$C = E_{DES}^{k3}\left(D_{DES}^{k2}\left(E_{DES}^{k1}(M)\right)\right)$$

- Variante de Carl Ellison :

$$C = E_{DES}^{k3}\left(T\left(E_{DES}^{k2}\left(T\left(E_{DES}^{k1}(M)\right)\right)\right)\right)$$

- Utilisation d'une fonction de transposition pour augmenter la diffusion ;

AES (Advanced Encryption Standard) ou Rijndael :

- Actuellement le chiffrement le plus utilisé et le plus sûr ;
- Bloc de 128 bits (16 octets) ;
- Clés de 128, 192 ou 256 bits
- Ce chiffrement n'a pas été cassé ;
- Recherche exhaustive (brute force) reste la seule solution ;
- La NSA utilise le chiffrement 128 bits pour des documents de niveau « SECRET », le niveau « TOP SECRET » utilise des clés de 192 ou 256 bits.

## AES (Advanced Encryption Standard) ou Rijndael :

• Fonctionnement :

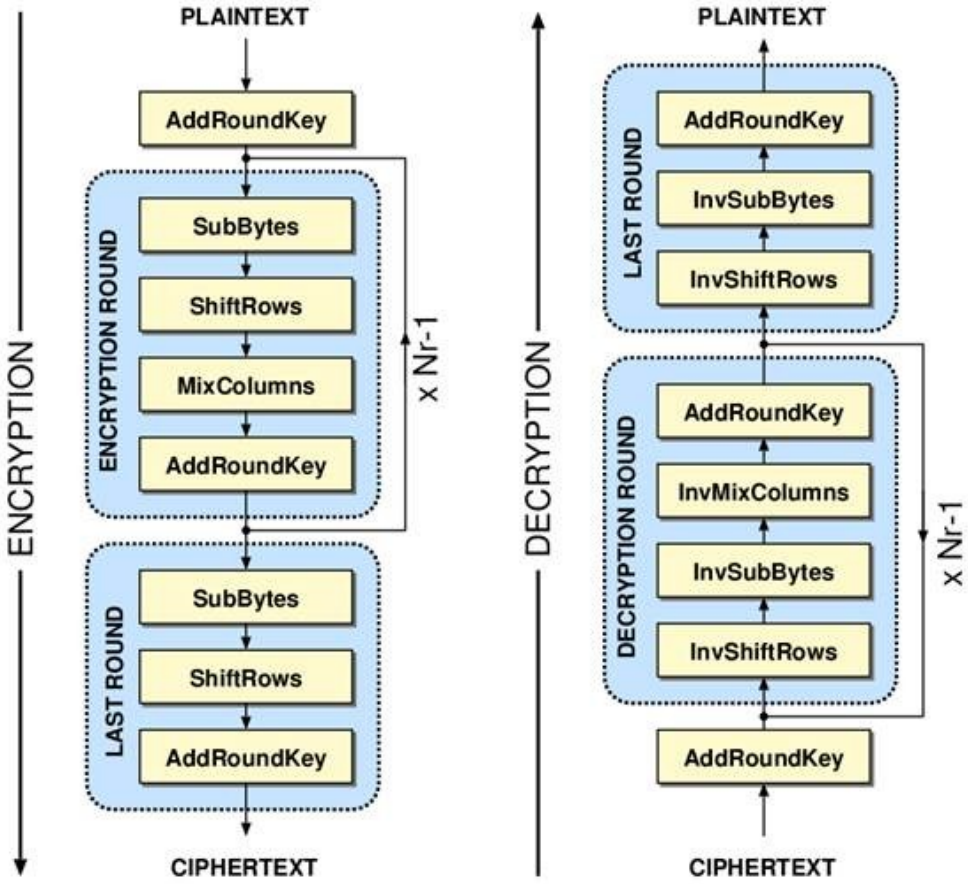
→ 16 octets sont placés dans une matrice 4x4 ;

→ rotation des lignes vers la droite ;

→ transformation linéaire appliquée (multiplication polynomiale) ;

→ XOR effectué avec une autre matrice ;

→ opération itérée 10, 12 ou 14 fois (clé de 128, 192 ou 256 bits).



# Chiffrements asymétriques

RSA (Rivest Shamir Adleman) :

• Algorithme complexe qui utilise plusieurs branches de l'arithmétique modulaire :

→ les congruences ;

a et b sont dits congrus modulo n si leur différence est divisible par n

a et b sont alors congrus modulo n si le reste de a par n est égal à celui de b par n

1) $26 \equiv 12\ (7) \rightarrow 26 - 12 = 14 \rightarrow$ 14 multiple de 7
2) 26 % 7 = 5 ET 12%7 = 5

→ le petit théorème de Fermat.

si p est un nombre premier et a est un entier, alors $a^p - a$ est multiple de p

• Pour obtenir des fonctions à sens unique avec brèche secrète (ou porte dérobée).

RSA (Rivest Shamir Adleman) :

- Principe de fonctionnement :

  → Les calculs se font modulo *P* ;
  (petit théorème de Fermat)

  → Les messages clairs et chiffrés sont des entiers inférieurs à *P* ;

  → Le message est élevé à une puissance modulo *P* ;
  (exponentiation modulaire)

- Il est essentiel que la génération du couple (de clés) soit vraiment aléatoire → pour ne pas retrouver la clé privée grâce à la clé publique !

- Les données à chiffrer ne doivent pas être trop courtes ;

Echange de clés Diffie Hellman (utilisé par SSH) :

• Algorithme qui utilise un cas particulier d'anneau commutatif : $\mathbb{Z}/n\mathbb{Z}$

• Les deux parties échangent :

→ un groupe ou corps fini ;
un groupe fini est déterminé par son cardinal qui est une puissance d'un nombre premier
→ un générateur de ce groupe.

• Ils décident d'un nombre secret qu'ils élèvent à une puissance issue du groupe ;

• Ils élèvent le nombre reçu à la puissance du nombre secret pour trouver la même clé ;



• comme il est difficile d'inverser l'exponentiation la clé est introuvable.

Echange de clés Diffie Hellman (utilisé par SSH) :

- Alice et Bob se mettent d'accord sur
  → le nombre premier p=11 ;
  → la base b=5.

- Alice choisit le nombre secret sa = **3** et Bob, sb = **9** ;

- Alice envoie à Bob $v_a = b^{sa} \bmod p$ soit $v_a = 5^3 \bmod 11 =$ **4**

- Bob envoie à Alice $v_b = b^{sb} \bmod p$ soit $v_b = 5^9 \bmod 11 =$ **9**

- Alice et Bob calculent la clé secrète :

  → $clé_a = (v_b)^{sa} \bmod p = 9^3 \bmod 11 =$ **3**
  → $clé_b = (v_a)^{sb} \bmod p = 4^9 \bmod 11 =$ **3**

Echange de clés Diffie Hellman (utilisé par SSH) :

Attaque :

- Ce protocole est vulnérable au MITM ;
- L'attaquant doit pouvoir intercepter p, b ,$v_a$ et $v_b$ ;
- Alice et Bob croient ainsi avoir échangé une clé ;
- En réalité ils ont chacun échangé une clé secrète avec l'attaquant ;

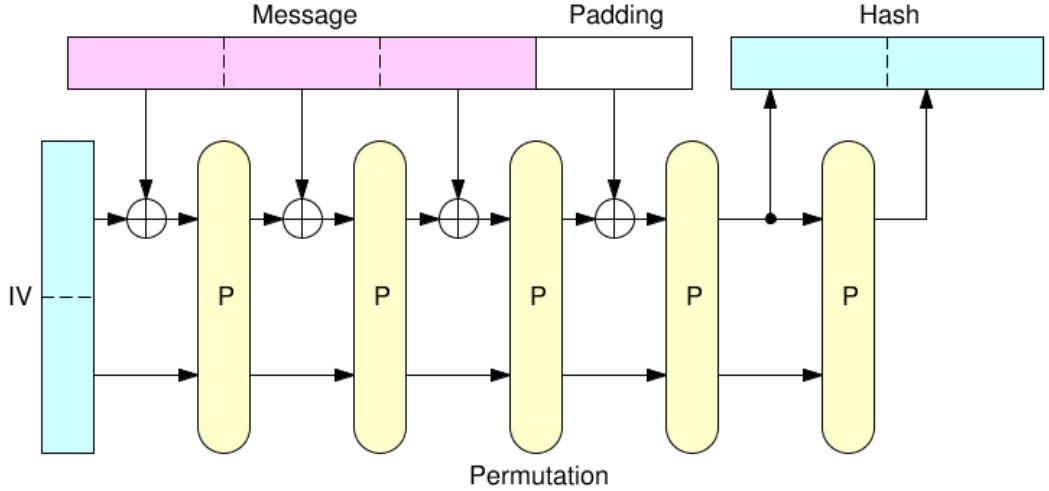
Parade :

- En SSH on utilise les fingerprints (challenge) ;
- On signe l'échange avec un couple asymétrique certifié.

# Fonctions de hachage

SHA (Secure Hash Algorithm) :

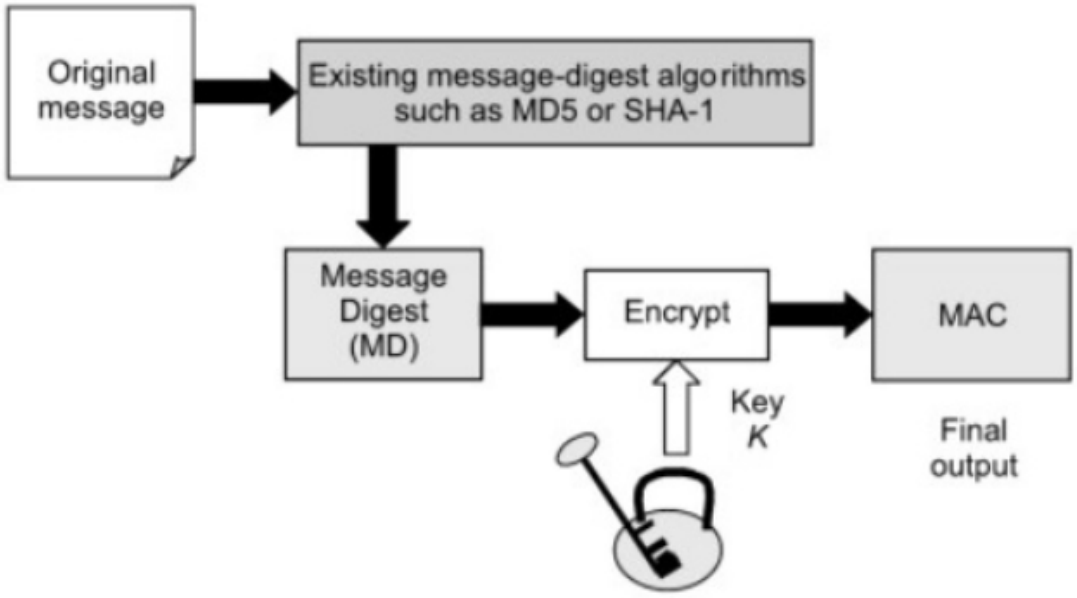
- Standard du gouvernement des États-Unis ;
- Développé par la NSA mais inspiration de MD5 (Ron Rivest) ;
- Principe :
  → la fonction prend en entrée un message de longueur variable ;
  → elle produit une empreinte ou haché de taille fixe ;
- Basé sur la construction de Merkle-Damgård :



K-HMAC (Keyed-Hash Message Authentication Code) :

- Type de Code d'Authentification de Message (CAM) ;
- Mixe une fonction de hachage avec une clé secrète ;
- Permet de vérifier l'intégrité **ET** l'authenticité d'un message ;
- La sécurité du HMAC dépend :

  → de l'algorithme de hash ;
  → de la taille de la clé.



# Un peu de cryptanalyse

Analyse fréquentielle :

• Examine les répétitions des lettres du message chiffré pour retrouver la clé de chiffrement ;

• Inefficace contre les chiffrements modernes (eg. RSA) ;

• Souvent utilisée conjointement avec l'indice de coïncidence (calcul de probabilité de répétition des lettres).

Attaque par dictionnaire :

• Teste tous les mots d'une liste comme clé de chiffrement ;

• Souvent couplé à la force brute pour l'accélérer ;

• Inefficace contre AES.

Cryptanalyse linéaire :

• Approximation linéaire de la structure interne du cryptosystème

• Efficace contre DES / inefficace contre les cryptosystèmes modernes ;

Cryptanalyse différentielle :

• Analyse statistique des modifications structurelles du cryptosystèmes en modifiant légèrement les entrées ;

• Nécessite un très grand nombre de perturbations pour récupérer la clé ;

• Inefficace contre AES.

Cryptanalyse par canal auxiliaire :

• Exploite une propriété « inattendue » de l'implémentation d'un cryptosystème ;

• Différents paramètres sont analysés : temps, bruit, consommation électrique ;

Cryptanalyse temps / mémoire :

• Souvent appelée table arc-en-ciel (rainbow table) ;

• Mélange entre l'attaque par force brute et l'attaque par dictionnaire :

→ force brute trop longue ;
→ dictionnaire trop de place en mémoire.