Introduction à la cryptographie

Techniques de Compression et utilisation d'outils Cryptographiques web et mobile

Birahime DIOUF, Docteur en Télécoms et Réseaux Enseignant chercheur

Chapitre 3 : Introduction à la cryptographie

Objectifs spécifiques : A la suite de ce chapitre, l'étudiant doit être en mesure de :

1. Décrire les mécanismes de cryptographie et
2. Connaitre les méthodes de cryptographie classique
3. Appliquer les techniques de cryptographie symétrique et non-symétrique
4. Maîtriser les algorithmes de chiffrement les plus couramment utilisés (DES, 3DES, IDEA, AES, RC4, RSA, DSA, …),
5. Comprendre la problématique liée à la cryptographie du futur (cryptographie quantique)
6. Savoir appliquer les techniques de cryptographie.

Chapitre 3 : Introduction à la cryptographie

Plan du chapitre :

- Sécurité de l'information
- Cryptographie
- Types et approches de la cryptographie
- Cryptographie symétrique
  - Méthodes de cryptographie classiques
  - Méthodes de cryptographie modernes
- Cryptographie asymétrique
- Problématique liée à la cryptographie du futur (cryptographie quantique)
- Applications des techniques de cryptographie.

Introduction à la sécurité

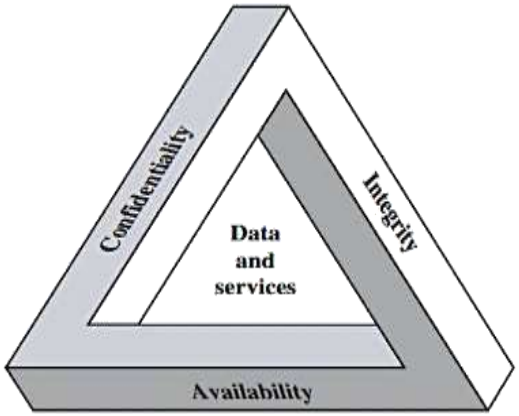
C'est quoi la sécurité, quoi sécuriser et pourquoi sécuriser

- Sécurité informatique : ensemble des moyens mis en œuvre pour réduire la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles.
- Développement de l'Internet ⟹ sécurité de l'information est aujourd'hui une véritable préoccupation pour les entreprises, opérateurs privés et administration.
- Les données financières et techniques échangées à travers internet sont souvent très convoitées et doivent être protégées.
- La confiance des utilisateurs passe par la sécurisation des transactions.
  - atteinte à l'image d'une entreprise,
  - perte de confiance de ses clients,
  - perte de recettes,
  - engagement de la responsabilité légale,
  - …

Introduction à la sécurité

Objectifs de la sécurité

- Pour limiter les vulnérabilités, la sécurité vise généralement les objectifs suivants :
  - La **confidentialité** consiste à assurer que seules les personnes autorisées ont accès aux ressources et empêcher toute divulgation non autorisée d'informations sensibles.
  - L'**intégrité** permet de se protéger contre toute modification non autorisée d'information.
  - La **disponibilité** vise à garantir à tout moment l'accès à un service ou à des ressources.

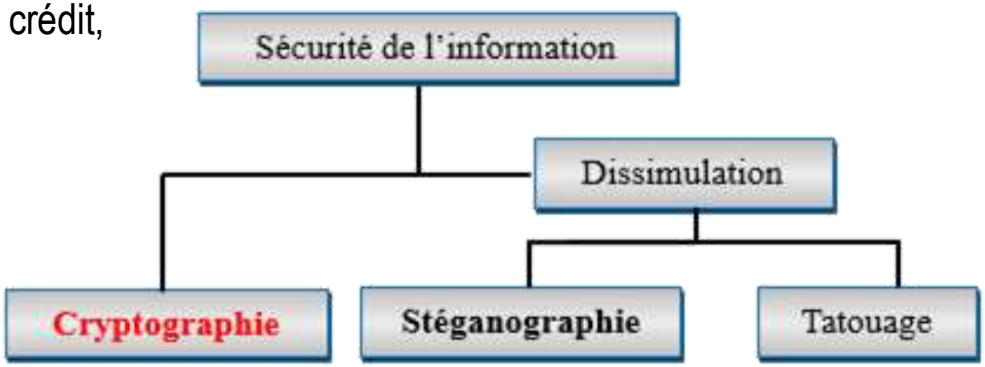


- Autres objectifs :
  - L'imputabilité est la possibilité d'attribuer une action à son auteur.
  - La non-répudiation permet de s'assurer qu'une transaction a effectivement eu lieu et qu'aucun des correspondants ne peut la nier.
  - L'audit permet l'enregistrement, le contrôle et l'évaluation de la sécurité.
  - Authentification est un des moyens qui permet de garantir la confidentialité.

Sécurité de l'information

Sécurisation de l'information

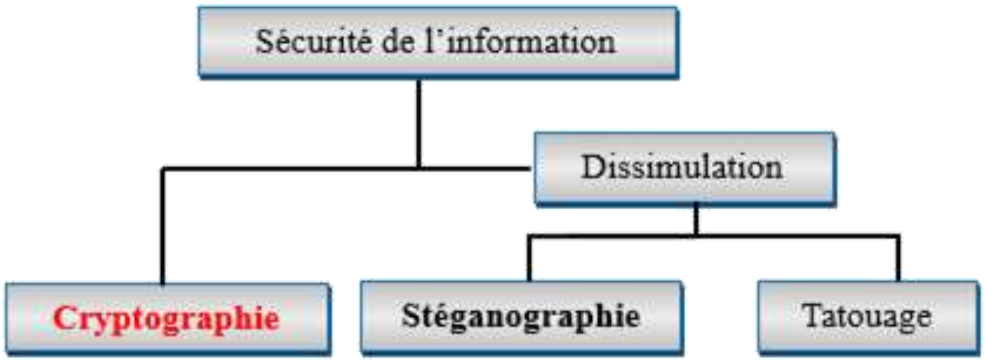
- Un canal de communication est généralement partagé par plusieurs entités.
- Pour qu'un émetteur puisse envoyer un message qui ne puisse être lu que par un destinataire spécifique, le message doit être *crypté* ou *dissimulé*.
- Dans le domaine de la transmission sécurisée de l'information on a :
- Cryptographie : étudie des codages et des protocoles permettant de communiquer des messages de manière secrète, de *signer* des documents ou d'*authentifier* un émetteur ;
  - essentielle à la sécurité des systèmes d'info. But : garantir la confidentialité, l'authenticité et l'intégrité des données échangées. Sans elle, un attaquant peut
    - écouter vos communications électroniques, par exemple en interceptant des requêtes HTTP ;
    - lire les fichiers du disque dur de votre ordinateur sans avoir votre mot de passe ;
    - retirer de l'argent avec votre carte de crédit,
    - …



Sécurité de l'information

Sécurisation de l'information

- Cryptanalyse : consiste à retrouver le message (texte en clair) sans connaître la clé.
  - chiffrement : algorithme E_k utilisé pour transformer un message en clair en message chiffré (cryptogramme).
  - déchiffrement : inverse du chiffrement D_k, transforme message chiffré en message en clair.
  - clé : secret partagé utilisé pour **chiffrer** et pour **déchiffrer**.
  - $D_k(E_k(m)) = m$.
- Stéganographie : cacher un message dans un contenu pour qu'il soit, non seulement indéchiffrable, mais imperceptible.
- Stéganalyse : art de déceler la présence d'un message caché.
- Tatouage : offre des solutions techniques pour faire face aux problèmes de protection des droits et des copies.



Types et approches de la cryptographie

Types de chiffrements

- Deux grands principes (types ou classes) de chiffrement (ou cryptage) :
  - le cryptage symétrique qui utilise une même clé partagée et
  - le cryptage asymétrique qui utilise deux clés distinctes.
- Deux méthodes (ou approches) de cryptage :
  - Transpositions qui mélangent l'ordre des symboles contenus dans le message et
  - substitutions qui remplacent un symbole par un autre.
    - ***substitution simple*** ou ***mono-alphabétique*** : consiste à remplacer chaque lettre du texte clair par une lettre, un signe ou un nombre.
    - ***substitution poly-alphabétique*** : consiste à changer une lettre par une autre, mais cette dernière n'est pas toujours là même.

Cryptographie symétrique (ou à clé secrète)

Méthodes classiques : substitution mono-alphabétique

- *Chiffre de César :* première technique de cryptographie alphabétique
  - chiffrement par décalage
  - Rang du décalage alphabétique = 3 : la lettre A est remplacée par D, B par E, …
  - Chiffre avec un algorithme (substitution) et une clé par décalage

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
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

  - **Exemple :** le mot CHAMPION est codé par FKDPSLRQ
  - D'autres variantes :
    - Décalage variables : ex : décalage de 4, 5, ….
    - avec décalage de 13 (algorithme ROT13), …
  - ***Exercice d'application :***
    1. Crypter votre prénom et décrypter le mot WURXYH avec César.
    2. Sachant que le texte clair RENDEZ VOUS donne MZIYZU QJPN déterminer la clé de cryptage.
    3. Décrypter le texte suivant en supposant que le mot "ENNEMI" y figure : STYWJ JSSJRN IJ YTZOTZWX JXY IJ WJYTZW.

Cryptographie symétrique

Méthodes classiques : substitution mono-alphabétique

- *Cryptage affine*
  - **Chiffrement** : à chiffrer chaque lettre, remplacer le nombre initial x par nombre y :
    $\boldsymbol{y = (ax + b)\ mod\ 26}$, avec $\boldsymbol{a, b \in [0, 25]}$ et $\boldsymbol{pgcd(a, 26) = 1}$
  - **Clé =** $\boldsymbol{(a, b)}$
  - **Déchiffrement** : remplacer y par nombre x :
  - $\boldsymbol{x = a^{-1}(y - b)\ mod\ 26}$, avec a^{-1} inverse de a modulo 26.
  - On attribue une valeur à chaque lettre de l'alphabet : 'A' = 0, 'B' = 1, … 'Z' = 25.

  - ***Exercice d'application:***

En clair	A	B	C	D
Rang x	0	1	2	3
ax + b		10		
Rang y		10		
En crypté		K		

    - Soit la clé affine (a ; b) = (3; 7).

    1. Chiffrer les lettres de l'alphabet en remplissant le tableau ci-contre :
    2. Coder votre prénom avec la clé (3;7)
    3. Décrypter la phrase RXF HPJJF avec la clé (3;7). Pour cette question vous avez besoin de calculer l'inverse de 3 (3^{-1}) en modulo 26. Voir la méthode de calcul d'inverse au diapo suivant.
    4. On considère la clé (5;7). Coder alors le mot ENTIER. Quel problème apparaît dans ce codage ?

Calcul d'inverse modulaire

- Deux nombres a et x sont inverses donc $ax = 1$.
- Si deux entiers a et x sont inverses modulo n alors $ax = 1\ mod\ n \iff ax = 1 + qn$, k étant un entier.

- **Exemple** : Calculons l'inverse de 9 en modulo 16. Soit x l'inverse de 9 en modulo 19.
  - $x = 9^{-1}\ mod\ 16 \Longrightarrow 9 \cdot x = 1\ mod\ 16 \Longrightarrow 9 \cdot x = 1 + 16 \cdot q$.
  - On itère sur $q = 1, 2, \ldots$ jusqu'à trouver un multiple de 9.
  - Pour $q = 1$, on a $9 \cdot x = 1 + 16 \cdot 1 = 17$ pas vrai car 17 n'est pas un multiple de 9.
  - Pour $q = 2$, on a $9 \cdot x = 1 + 16 \cdot 2 = 33$ pas multiple de 9.
  - Pour $q = 3$, on a $9 \cdot x = 1 + 16 \cdot 3 = 49$ pas multiple de 9.
  - Pour $q = 4$, on a $9 \cdot x = 1 + 16 \cdot 4 = 65$ pas multiple de 9.
  - Pour $q = 5$, on a $9 \cdot x = 1 + 16 \cdot 5 = 81$ pas vrai car 81 est bien un multiple de 9.
  - Ainsi $9 \cdot x = 81$ donc $x = 9$. D'où $9 = 9^{-1}\ mod\ 16$.

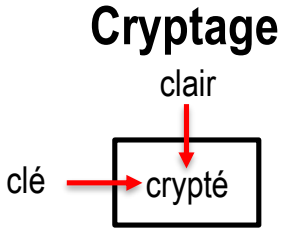
Cryptographie symétrique

Méthodes classiques : substitution poly-alphabétique

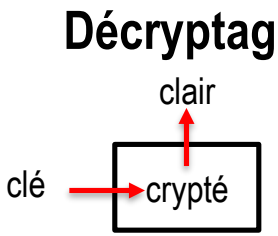
- *Chiffre de Vigenère*
  - C'est un César à décalage variable dépendant d'une clé numérique.
  - Basée sur une *Table de Vigenère* : chiffrement se déroule en 2 étapes :
    - **Exemple** : message = « WEB ET MOBILE » et clé = « UVS »

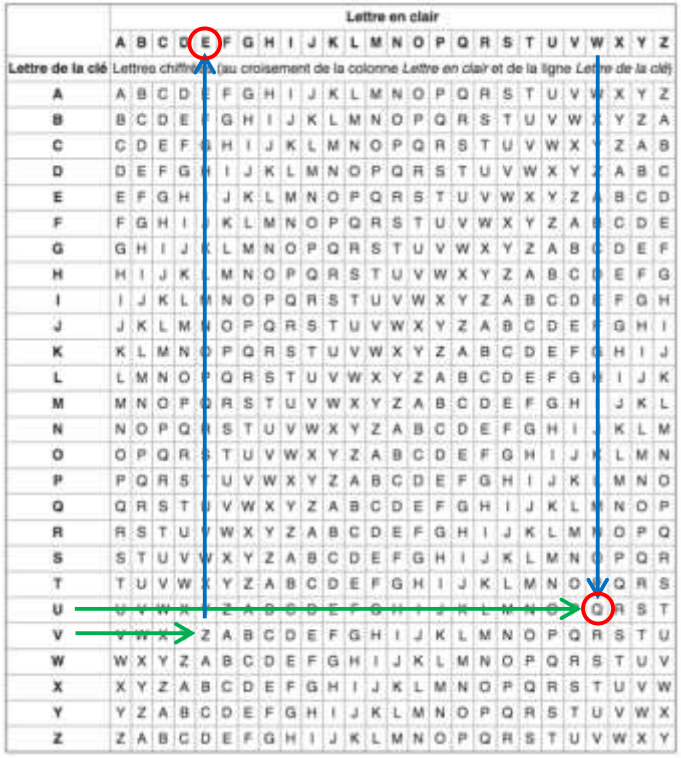
Pour le cryptage (resp. décryptage), en-dessous de chaque lettre du message (resp. cryptogramme), on écrit chaque lettre de la clé, en répétant le motif autant de fois que nécessaire.

➢ **Cryptage :**
- Message clair : WEB ET MOBILE
- Clé : UVS UV SUVSUV
- Message crypté : QZT YO EIWAFZ



➢ **Décryptage :**
- Cryptogramme : QZT YO EIWAFZ
- Clé : UVS UV SUVSUV
- Message décrypté : WEB ET MOBILE





UVS
UNIVERSITE VIRTUELLE DU SENEGAL

Cryptographie symétrique

Méthodes classiques : substitution poly-alphabétique

- *One Time Pad (Masque jetable ou chiffre de Vernam)*
  - Propriétés de la clé pour garantir une sécurité optimale (incassable).
    - le nombre de caractères de la clé doit être supérieur ou égal à celui du message ;
    - les caractères de la clé doivent avoir été choisis de manière aléatoire ;
    - chaque clé ne doit être utilisée qu'une seule fois.
  - Si elles sont respectées à la lettre, la sécurité garantie est *absolue*.
  - **Exemple :**
    - Message de 4 lettres : ZERO.
    - Une clé de 4 lettres au hasard : JRVG.
    - On attribue une valeur à chaque lettre de l'alphabet : 'A' = 0, 'B' = 1, … 'Z' = 25.

Chiffrement : $LettreChiffrée = (LettreMessage + LettreClé)\ mod\ 26$

Déchiffrement : $LettreDéchiffrée = (LettreChiffrée - LettreClé)\ mod\ 26$

Chiffrement :

- ✓ Z + J = 25 + 9 = 34 - 26 = 8 = I
- ✓ E + R = 4 + 17 = 21 = V
- ✓ R + V = 17 + 21 = 38 – 26 = 12 = M
- ✓ 0 + G = 14 + 6 = 20 = U

Message chiffré : IVMU

Message déchiffré : ZERO

Déchiffrement :

- ✓ I - J = 8 - 9 = -1 + 26 = 25 = Z
- ✓ V - R = 21 - 17 = 4 = E
- ✓ M - V = 12 - 21 = -9 + 26 = 17 = R
- ✓ U - G = 20 - 6 = 14 = O

Cryptographie symétrique

Méthodes classiques : transposition

- *Transposition rectangulaire*
  - Ecrire la clé sur la première ligne de la grille rectangulaire;
  - écrire le message dans les lignes suivantes de la grille rectangulaire,
  - puis Trie les colonnes de cette grille selon l'ordre alphabétique des lettres de la clé.
  - Après avoir rempli la grille, s'il reste des cases vides, on peut les remplir avec des nulles (ici X).
  - ***Exemple :***
    - K = INFO, p = 4
    - M = CRYPTOGRAPHIE

Tri dans l'ordre alphabérique de la clé

I	N	F	O
C	R	Y	P
T	O	G	R
A	P	H	I
E	X	X	X

F	I	N	O
Y	C	R	P
G	T	O	R
H	A	P	I
X	E	X	X

D'où le message chiffré est

C = YGHXCTAEROPXPRIX

  - **NB** : Dans le cas ou la clé est donnée en chiffre, le message est écrit en fonction de la taille de la clé et tableau arrangé selon la clé (l'ordre de lecture les colonnes)

Cryptographie symétrique

Méthodes modernes : modes de chiffrements

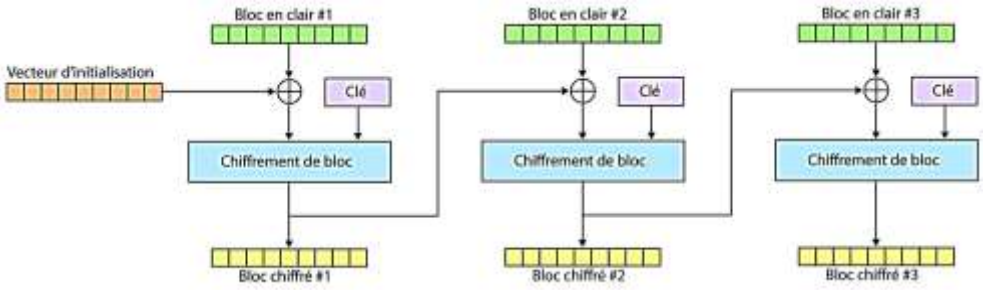
- 2 modes de chiffrements utilisés par les algorithmes contemporains :
  1. Cryptages par blocs :
     - Le message binaire à chiffré est d'abord est découpé en blocs de taille fixe généralement identique à la taille de la clé (64 ou 128 ou 256 bits).
     - chiffrent les différents blocs clairs suivant le mode.
  2. Cryptages par flot en continu (*stream*) :
     - chiffrent les octets au fur et à mesure, sans attendre la réception complète des données à crypter et sans contrainte de taille.
     - algorithmes en général coûteux et dépendent des conditions d'utilisation du chiffre dans la liaison.
- Plusieurs approches (modes) :
  - *Electronic Code Book (ECB)*
  - *Cipher Block Chaining (CBC)*
  - *Cipher Feedback (OFB)*
  - *Output Feedback (OFB)*
  - *Counter (CTR)*

Cryptographie symétrique

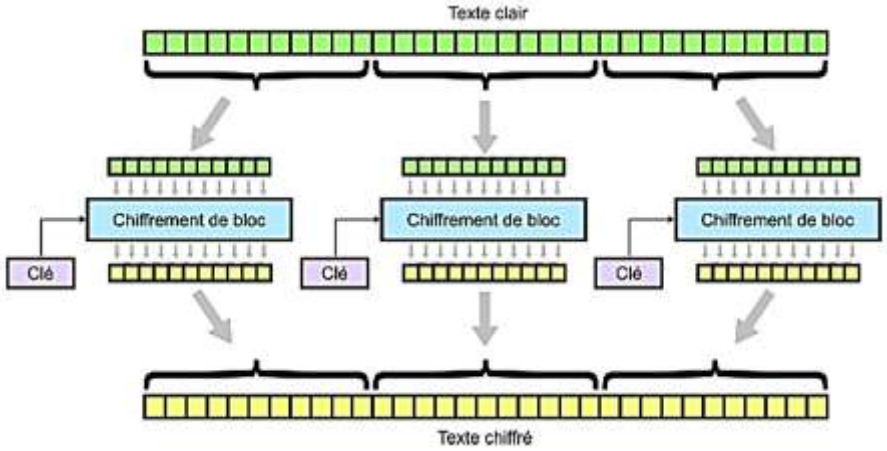
Méthodes modernes : modes de chiffrements

- *Mode ECB (Electronic Code Book)*
  - 2 blocs clairs identiques produisent le même bloc chiffré ⟹ on peut détecter des motifs répétés
  - Avantage : calcul simultané et rapide des blocs chiffrés.
- *Mode CBC (Cipher Block Chaining)*
  - Plus efficace que ECB car impossible de détecter des motifs répétés.
  - Inconvénient : risque de propagation d'erreur ; une erreur affectant un bloc reçu se répercutera sur le déchiffrement des blocs suivants. De plus le calcul doit être réalisé bloc par bloc.
  - On applique au 1er bloc un IV (Vecteur d'Initialisation) choisi de manière aléatoire et transmis avec le message chiffré.

CBC



ECB



UVS
UNIVERSITE VIRTUELLE DU SENEGAL

Cryptographie symétrique

Méthodes modernes : modes de chiffrements

- *Exemple mode ECB et CBC*
  - Soient message clair m=101100010100101 et la clé K=(1->2, 2->3, 3-> 4, 4->1) par permutation (c-à-d le chiffrement consiste à décaler à gauche les éléments du bloc de 4bits.
    1. Chiffrez le message m avec le mode ECB.
    2. Chiffrez le message m avec le mode CBC. Prendre VI = 1010 vecteur d'initialisation.
  - ***Correction :***
    - Tout d'abord, on découpe le message m en bloc de taille 4 (d'après la clé).
    - m = 101100010100101 $\Rightarrow m_1$ = 1011 ; m_2 = 0001 ; m_3 = 0100 ; m_4 = 1010.
    - Puis bourrage du dernier bloc en lui ajoutant un seul 0 pour avoir que des blocs de taille 4.

1. Pour ECB, $c_i = E_k(m_i)$

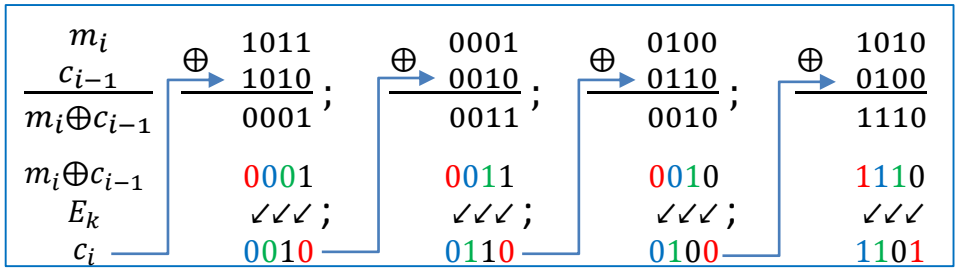
Les blocs sont chiffrés séparément.

m_i	1011	0001	0100	1010
E_k	↙↙↙ ;	↙↙↙ ;	↙↙↙ ;	↙↙↙
c_i	0111	0010	1000	0101

décaler à gauche

$\Longrightarrow$ message chiffré c = 0111001010000101

2. Pour CBC, $c_i = E_k(m_i \oplus c_{i-1})$ avec $c_{-1} = IV$



$\Longrightarrow$ message chiffré c = 0010011001001101

Cryptographie symétrique

Méthodes modernes : modes de chiffrements

- *Mode ECB et CBC*
  - Le mode ECB comporte cependant un défaut de taille : **tous les blocs en clair identiques vont donner le même bloc chiffré.**
  - Cela est particulièrement visible pour une image.
  - Tous les pixels sont chiffrés, mais chaque pixel identique donnera le même pixel chiffré, et le motif de l'image est toujours visible dans le texte chiffré.
  - Ce qui n'est pas le cas pour CBC

image non chiffrée

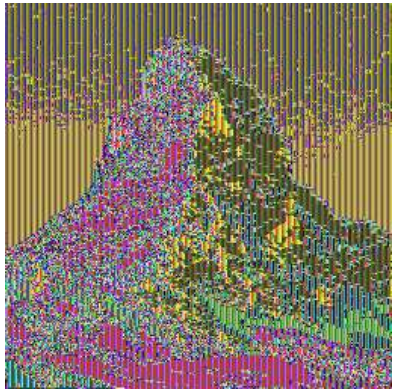


image chiffrée en mode ECB

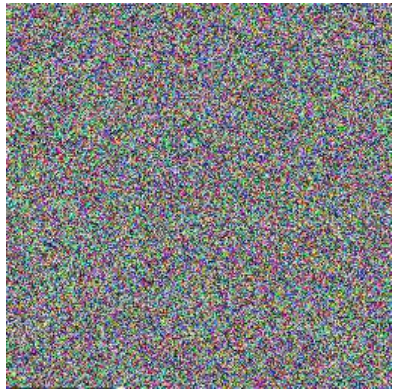
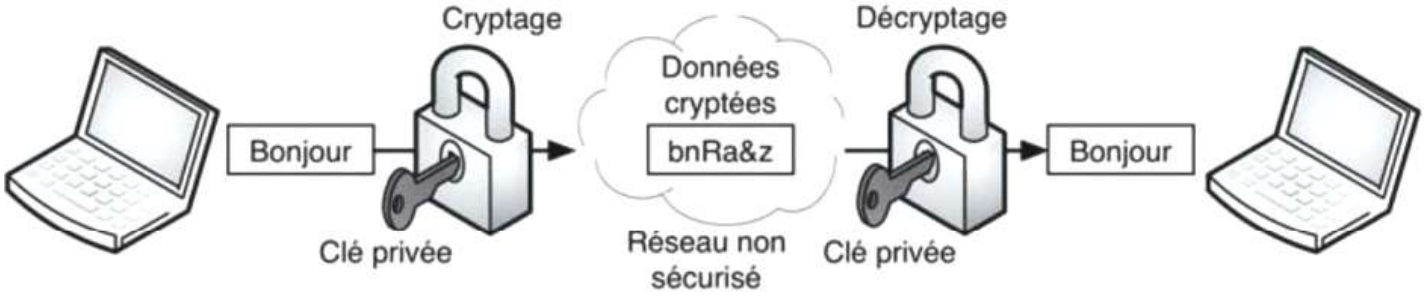


image chiffrée en mode CBC

Cryptographie symétrique

Méthodes modernes :

- Pour la cryptographie symétrique (ou cryptographie à clé secrète), la même clé sert à crypter et à décrypter les messages.
- Clé secrète est partagée entre les deux parties communicantes.
- Avantages : chiffrement efficace (longueurs de clés de 64 ou 128 bits suffisantes), rapide et peu gourmand en puissance de calcul.
- Difficulté : *trouver un moyen sécurisé pour communiquer la clé aux deux entités*.
- Les risques de pertes et de vols sont aussi à considérer, il faudra donc la renouveler souvent.
- Choix de la clé secrète : souvent réduit à un mot de passe alphanumérique.
- Indication : choisir un mot de passe complexe n'appartenant à aucun dictionnaire.



Cryptographie symétrique

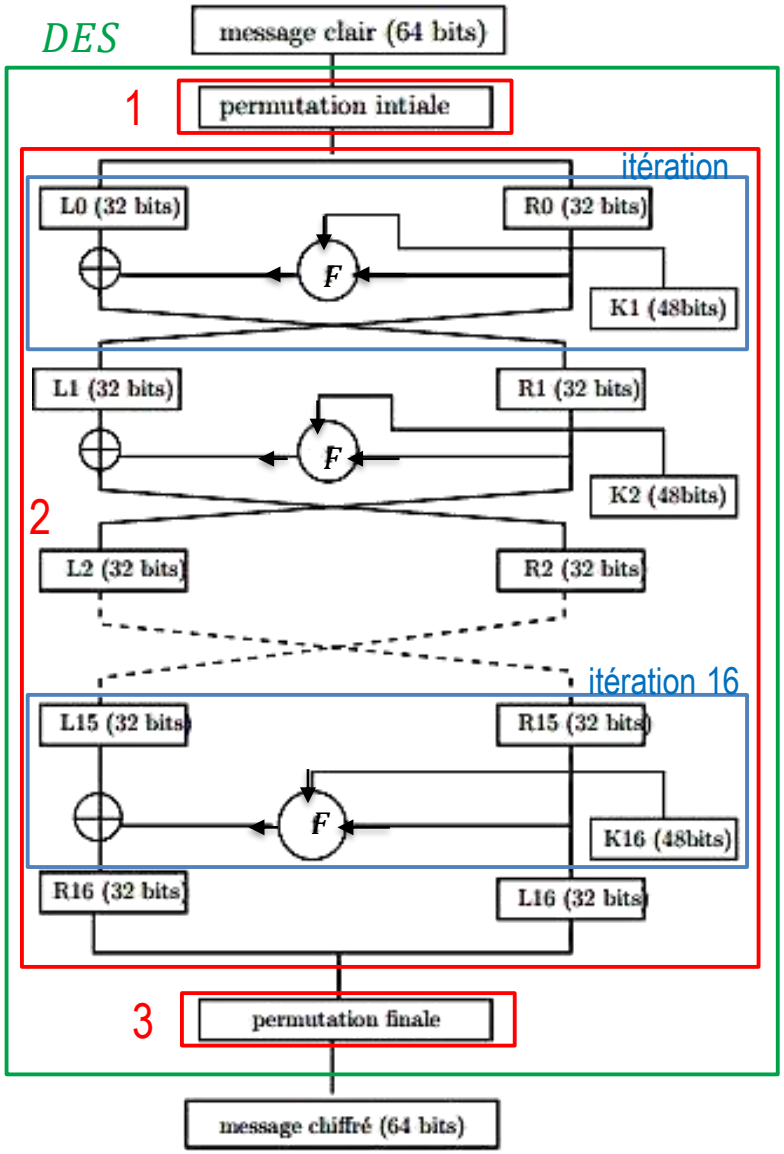
Méthodes modernes : algorithmes

Nom de l'algorithme	Clés utilisées	Propriétés de l'algorithme
DES (Digital Encryption Standard)	56 bits	Issu d'IBM Lucifer, adopté comme standard par la NSA en 1976 sa robustesse est mise en cause, chiffrement par blocs de 64 bits
3DES	168 bits	Triple DES, Application de DES 3 fois successives,
AES (Advanced Encryption Standard) ou RijDael	128, 192, ou 256 bits	Successeur de DES depuis 2000 élu standard par la NIST (National Institute of Standards and Technology, USA), le plus efficace, Chiffrement par blocs de 128 bits
Blowfish	256 à 448 bits	Output feedback Chiffrement par bloc très rapide
RC 2-4-5-6 (Rivest's Cipher)	variable	Issu de RSA Security Inc. Chiffrement par flux très rapide et simple, peu sûr
IDEA (International Data Encryption Algorithm)	128 bits	IDEA (International Data Encryption Algorithm) propriété de MédiaCrypt société suisse, utilisé dans PGP Chiffrement par blocs de 64 bits

Cryptographie symétrique

Méthodes modernes : DES

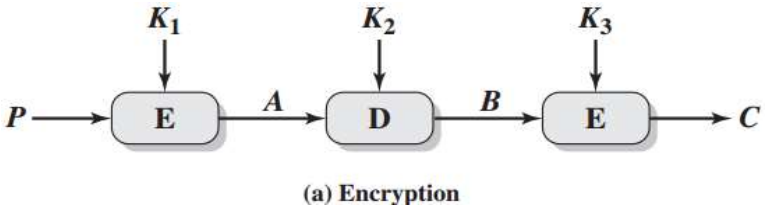
- Haut niveau de sécurité (en son temps), l'entière sécurité de l'algorithme repose sur les clés puisque l'algorithme est parfaitement connu de tous.
  - Clé de longueur de 64 bits (8 caractères) dont seulement 56 bits sont utilisés.
  - Utilisée pour générer 16 autres clés (Ki) de 48 bits pour les 16 itérations du D.E.S.
- DES ⟹ succession d'opérations en 3 étapes :
  1. Permutation initiale
  2. Calcul médian (16 itérations) :
     - Chaque bloc de 64 bits est découpé en 2 demi-blocs (de 32 bits) et chacun subit une série d'opérations.
     - F : fonction assurant une opération non linéaire de substitution sur le bloc d'entrée.
     - La sortie de F est xorisée avec l'autre demi-bloc.
  3. Permutation finale



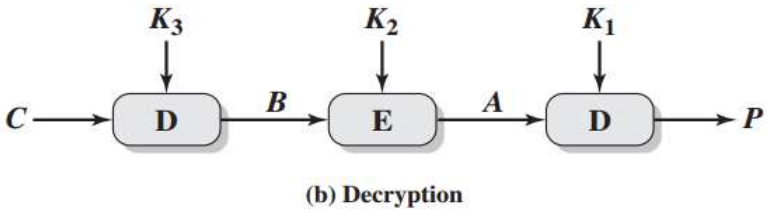
Cryptographie symétrique

Méthodes modernes : 3DES (triple DES)

- Progression de la puissance des ordinateurs a causé la mort du DES.
- DES n'est plus jamais utilisé lorsque la sécurité demandée est forte (utilisation militaire, documents secrets, etc.) $\Longrightarrow$ des améliorations sont nécessaires.
- Faiblesses liées à la taille de la clé de DES ont conduit à une version plus robuste triple DES (3DES) = enchaînement de 3 DES successifs avec 3 clés différentes.
- Il existe différentes approches de cette concaténation



(a) Encryption



(b) Decryption

$$C = E\big(K_3, D(K_2, E(K_1, P))\big)$$

$$P = D\big(K_1, E(K_2, D(K_3, C))\big)$$

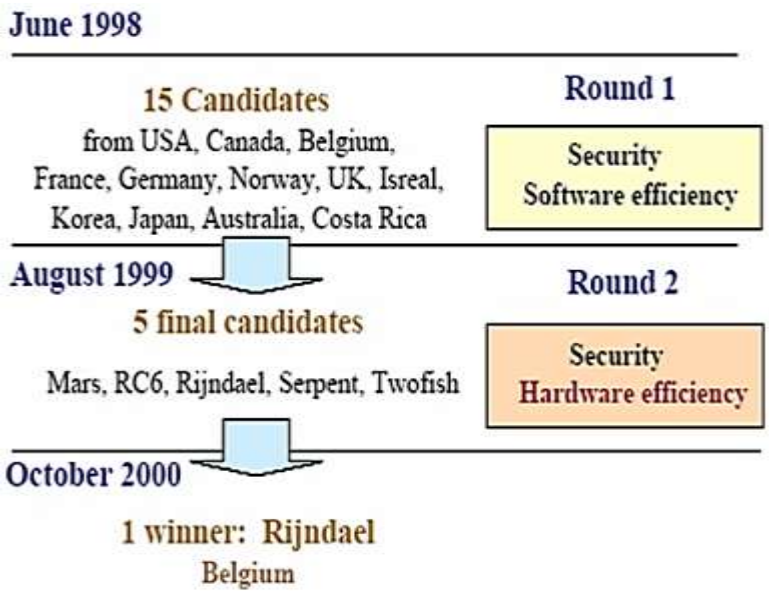
- Il était très robuste contre toutes les attaques faisables connues.
- Cependant, il est beaucoup plus lent que le DES car on triple les opérations.

Cryptographie symétrique

Méthodes modernes : AES

- AES ou Rijndeal (Rijmen and Deamen) issu d'un concours international NIST.
- 3DES demeure toutefois une norme acceptée aux U.S.A.

Déroulement du concours AES



- **Cahier des charges :** critères de sélection :
  - Clé de longueur de 64 bits.
  - sécurité générale,
  - coût en terme de calculs (rapidité),
  - simplicité de l'algorithme et ses facilités d'implémentation,
  - lecture facile de l'algorithme, puisqu'il est destiné à être rendu public,
  - résistance aux attaques connues,
  - flexibilité/portabilité : destiné à servir dans les cartes à puces, …

Cryptographie symétrique

Méthodes modernes : AES

- **Avantages et limites**
- Suite à une analyse de la NSA, le gouvernement américain a annoncé à propos de l'algorithme AES :
  - pour protéger des documents classifiés niveau « SECRET » : l'architecture et la longueur de toutes les tailles de clés de l'algorithme AES (128, 192 et 256) sont suffisantes.
  - Le niveau « TOP SECRET » nécessite des clés de 192 ou 256 bits.
  - L'implémentation de l'AES dans des produits destinés à la protection des systèmes et/ou documents liés à la sécurité nationale doit faire l'objet d'une analyse et d'une certification par la NSA avant leur acquisition et leur utilisation.

Cryptographie symétrique

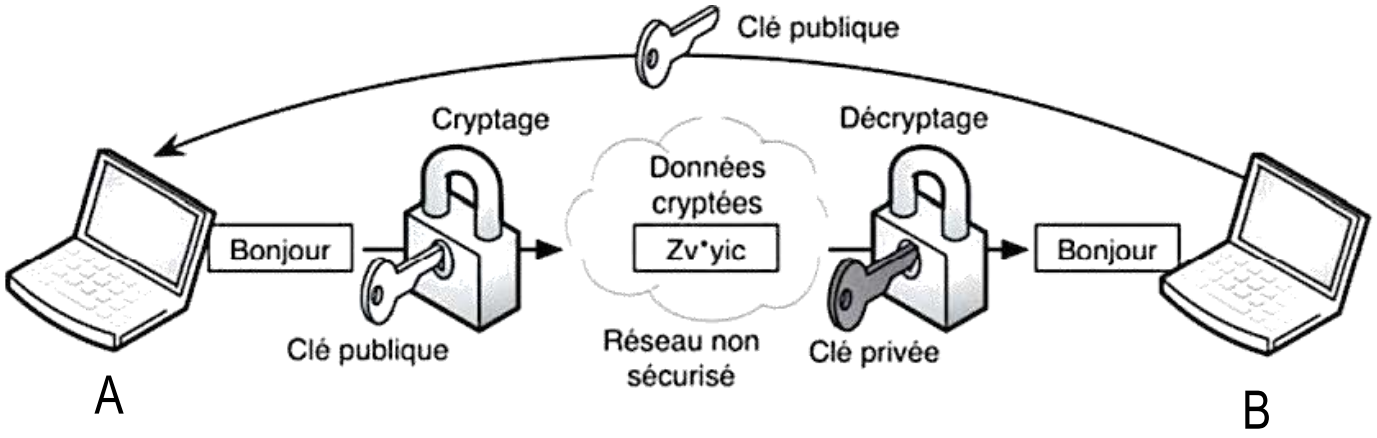
Méthodes modernes : AES

- **Avantages et limites**
- Les principaux avantages sont :
  - possibilité de réalisation en "Smart Card" (carte à puce) avec peu de code,
  - possibilité de parallélisme, $\Longrightarrow$ coût en terme de calculs réduit,
  - Ne comprend pas d'opérations arithmétiques : uniquement des décalages et des XOR,
  - n'utilise pas de composants d'autres crypto-systèmes,
  - nombre de rondes facilement augmenté si c'est requis (nombre de tours 10, 12 ou 14 selon la taille de la clé)
  - pas de clés faibles, techniquement, chiffrement par blocs de 128 bits, clés de 128, 192 ou 256 bits.
  - résistant à la cryptanalyse différentielle et linéaire,
  - ...
- Il possède pourtant quelques inconvénients et limites :
  - code et tables différents pour le chiffrement et déchiffrement,
  - déchiffrement plus difficile à implanter en "Smart Card", …
- **Attaques**
  - AES sensible à certaines attaques par canal auxiliaire, n'impliquant pas directement l'algo.
  - il est fort probable qu'à moyen terme, l'AES soit mis à mal.

Cryptographie asymétrique (à clé publique)

Introduction

- Principe :
  - le cryptage asymétrique utilise deux clés distinctes
    - La ***clé publique*** utilisée lors du chiffrement et
    - La ***clé privée*** utilisée pour le déchiffrement.



- La paire de clés utilisée est celle de récepteur B.

Cryptographie asymétrique

Introduction

- Algorithmes :
  - L'algorithme de chiffrement asymétrique le plus courant est l'algorithme *RSA* (*Rivest-Shamir-Adleman*).
  - L'algorithme *ElGamal* : basé sur les logarithmes discrets. Il est également très utilisé pour le chiffrement et la signature.
  - Le programme complet de cryptographie à clé publique le plus connu est *PGP* (*Pretty Good Privacy*).
  - Le format *OpenPGP* est le standard ouvert de cryptographie issu de PGP.

Nom de l'algorithme	Clés utilisées
RSA	1024 à 2048
El Gamal	160 à 1024

Cryptographie asymétrique

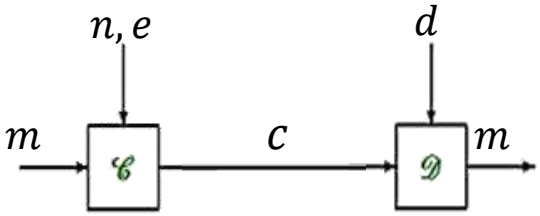
Algorithme RSA

- RSA est fondé sur la difficulté de factoriser des grands nombres qui sont le produit de deux grands nombres premiers.

- Procédure :
  - on chiffre le message avec une clé symétrique,
  - Choisir deux nombres premiers $\boldsymbol{p}$ et $\boldsymbol{q}$, les deux étant plus grands que 2^{10}.
  - Calculer $n = p \cdot q$ (n est le modulus) et $\varphi(n) = (p-1) \cdot (q-1)$ (fonction d'Euler)
  - Choisir $\boldsymbol{e}$ aléatoire premier avec $\varphi(n)$ ($pgcd(e, \varphi(n)) = 1$).
  - Trouver $\boldsymbol{d}$ tel que : $e * d = 1\ mod(\varphi(n))$ (c-à-d $d = e^{-1}\ mod(\varphi(n))$).
  - Clé publique : (n, e).
  - Clé privée : (n, d) ou (p, q, d) si on désire garder p et q.

Chiffrement :

$$c = m^e\ mod(n)$$



Déchiffrement:

$$m = c^d\ mod(n)$$

m : message et c : message chiffré

Cryptographie asymétrique

Algorithme RSA

- **Exemple** : Soit $\boldsymbol{p = 3}$ et $\boldsymbol{q = 11}$
  - on a donc $\boldsymbol{n} = p * q = \boldsymbol{33}$;
  - Ainsi, $\boldsymbol{\varphi(n)} = (p-1) * (q-1) = 2 * 10 = \boldsymbol{20}$;
  - On choisit aléatoirement $\boldsymbol{e = 3}$, qui n'a pas de facteur commun avec 20.
  - On cherche $d = e^{-1} mod\ (20)$, soit $\boldsymbol{d = 7}$.
  - Chiffrer le message "ASSEZ" en codant A=0, B=1, …, Z=25.

Message clair	Valeur	m^3	Message chiffré $c = m^3\ mod(33)$	c^7	$m = c^7\ mod(33)$	Caractère Déchiffré
A	0	0	0	0	0	A
S	18	5832	24	4 586 471 424	18	S
S	18	5832	24	4 586 471 424	18	S
E	4	64	31	27 512 614 111	4	E
Z	25	15625	16	268 435 456	25	Z

Chiffrement — déchiffrement

Cryptographie asymétrique

Algorithme RSA

- Pour un cryptanalyste, retrouver la clef privée à partir de la clef publique nécessite de connaître $\varphi(n) = pq$, donc de connaître p et q. Pour cela, il doit factoriser n.
- Donc n doit être suffisamment grand pour que cela ne soit pas possible dans un temps raisonnable par rapport au niveau de sécurité requis.
- Actuellement, la longueur du module n varie généralement de 512 à 2048 bits suivant les utilisations.
- Compte tenu de l'augmentation des vitesses de calcul des ordinateurs et des avancées mathématiques en matière de factorisation des grands nombres, la longueur minimale des clés doit augmenter au cours du temps.

- **NB** : L'algorithme RSA peut être utilisé pour
  - l'échange de clés symétriques.
  - la signature électronique (nous l'aborderons dans la séquence 4).

Cryptographie asymétrique

Echange de clés symétriques

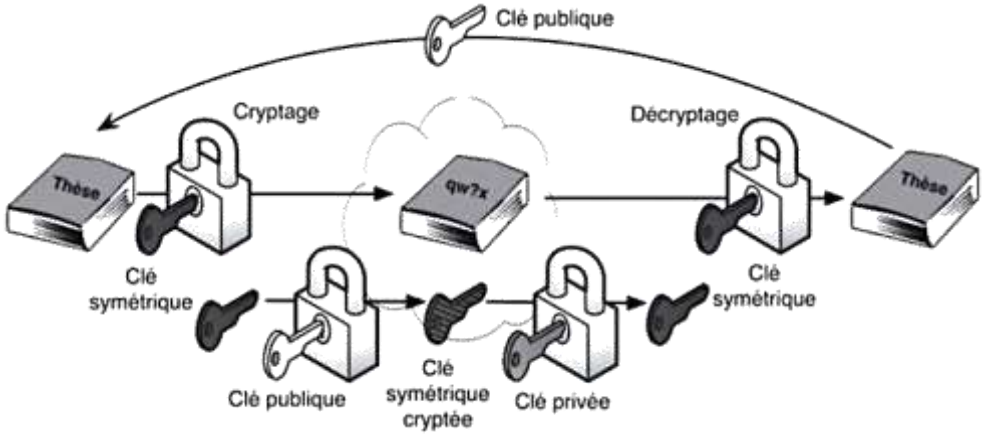
- Deux méthodes pour résoudre l'échange de clé symétrique :
  1. Utilisation du chiffrement symétrique (RSA par exemple) ;
  2. Méthode de DH (Diffie-Hellman).

1. Utilisation du chiffrement asymétrique

- Procédure :
  - on chiffre le message avec une clé symétrique,
  - on chiffre la clé symétrique avec la clé publique du destinataire,
  - on joint la clé symétrique chiffrée au message,
  - le destinataire déchiffre la clé symétrique avec sa clé privée, puis le message avec la clé symétrique qu'il peut utiliser à son tour pour envoyer des messages chiffrés ;

➢ Principale faiblesse :

✓ la clé symétrique cryptée est transmise sur le réseau et donc susceptible d'être interceptée et déchiffrée;

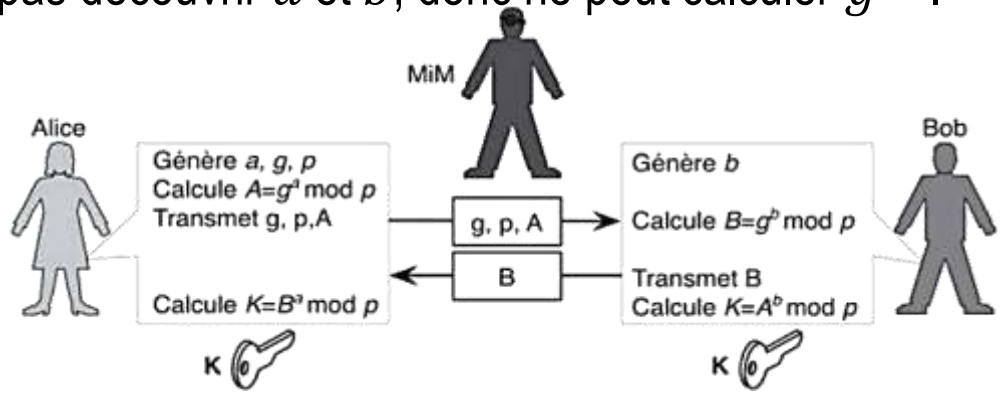


Cryptographie asymétrique

Echange de clés symétriques

2. Utilisation de la méthode de Diffie-Hellman (DH)

- Notamment utilisé dans le protocole SSH
- Clé symétrique générée par les deux extrémités; pas nécessaire de la transmettre.
- Procédure :
  - Alice et Bob ont choisi un groupe de nombres et une génératrice g de ce groupe,
  - Alice choisit un nombre au hasard a, élève g à la puissance a, et transmet g^a à Bob,
  - Bob fait de même avec le nombre b et transmet g^b à Alice,
  - Alice, en élevant le nombre reçu de Bob à la puissance a, obtient g^{ba} et la clé K,
  - Bob fait le calcul analogue et obtient g^{ab}, et donc la même clé K.
- Il est très difficile d'inverser l'exponentiation dans un corps fini.
- *MiM* (*Man in the Middle*) ne peut pas découvrir a et b, donc ne peut calculer g^{ab}.



UVS
UNIVERSITE VIRTUELLE DU SENEGAL

Machines quantiques et cryptographie quantique

Problématique liée aux machines quantiques et cryptographie du futur

- Un calculateur ou ordinateur quantique utilise les propriétés quantiques de la matière pour effectuer des opérations sur des données. À la différence d'un ordinateur classique basé sur des transistors travaillant sur des données binaires (0/1), l'ordinateur quantique travaille sur des qubits dont l'état quantique peut posséder une infinité de valeurs.
- La sécurité d'un algorithme de cryptographie est mesurée par le temps que prendrait un ordinateur pour faire la cryptanalyse. Ce temps s'estime en milliards d'années avec les ordinateurs classiques pour les algorithmes comme RSA.
- Or, l'accélération des capacités de calcul permise par l'ordinateur quantique permettrait de rendre la cryptanalyse beaucoup plus rapide que par un ordinateur classique.
- $\Longrightarrow$ Nécessaire de trouver une nouvelle cryptographie pour résister aux attaques des ordinateurs quantiques : c'est la cryptographie quantique qui utilise la mécanique quantique : sécurité garantie non par des théorèmes mathématiques, mais par les lois fondamentales de la physique comme le principe d'incertitude d'Heisenberg qui affirme que certaines quantités ne peuvent pas être mesurées simultanément. Dans le transport de clé "quantique", l'info est transportée par les photons (composants élémentaires de la lumière) polarisés.