Sécurité Informatique

Cryptographie

F.Z. Filali

Mars 11, 2018

Plan

Introduction

- Depuis 3000 ans environ, les êtres humains ont tenu à garder secret certaines conversations.
- La cryptographie était le domaine réservé des services du chiffre chez les militaires, du code de César à la machine Enigma.
- Elle fait aujourd'hui partie de notre vie quotidienne : cartes à puce et monétique, Internet et courrier électronique ...
- Nous faisons déjà tous de la cryptographie sans le savoir.

Vocabulaire de base

- **Texte en clair** : l'objet (texte, document, image, ...) à chiffrer.
- **Texte chiffré** : résultat du chiffrement.
- **Chiffrement** : processus à travers lequel un texte en clair est converti en un texte chiffré.
- **Algorithme de chiffrement** : étapes de traitement des données permettant de transformer un texte en clair en un texte chiffré.
- **Clé secrète (chiffre)** : paramètre utilisé par l'algorithme de chiffrement.
- **Déchiffrement** : processus permettant d'obtenir le texte en clair à partir du texte chiffré.
- **Algorithme de déchiffrement** : étapes de traitement des données permettant de transformer un texte chiffré en un texte en clair.

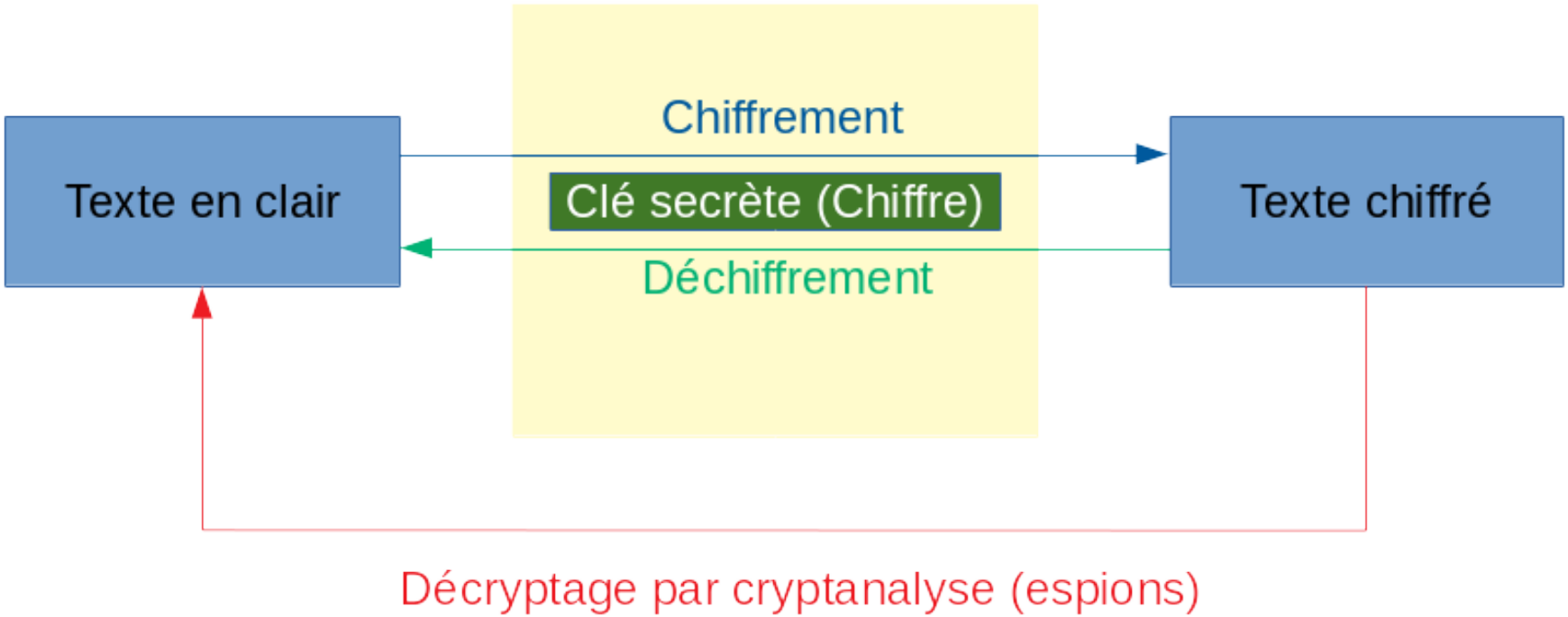
Vocabulaire de base

- **Cryptographie** : schémas et mécanismes disponibles pour le chiffrement et le déchiffrement.
- **Système cryptographie (cryptosystème)** : un schéma ou mécanisme singulier de chiffrement.
- **Cryptogramme** : texte chiffré à l'aide d'un cryptosystème.
- **Chiffrement par bloc** : transformation à la fois d'un bloc de données en entrée en un bloc chiffré de la même taille.
- **Chiffrement par flot** : chiffrement des données à la volée et n'a pas besoin de les découper.

Vocabulaire de base

- **Cryptanalyse** : signifie "casser un code". Elle se base sur la connaissance de l'algorithme de chiffrement et une certaine connaissance de la structure probable du texte en clair. Ceci afin de reconstruire partiellement ou totalement le texte en clair à partir du texte chiffré ou déduire la clé de déchiffrement.
- **Cryptologie** : science qui regroupe la **cryptographie** et la **cryptanalyse**.
- **Espace des clés** : nombre total de toutes les clés possible pouvant être utilisées dans un système cryptographie.

Vocabulaire de base



Cryptographie

- Cryptographie classique
  - Substitution (César, Vigenère, Polybe, Hill)
  - Transposition (ADGFX)
- Cryptographie moderne
  - Symétrique: à clé secrète (DES, AES)
  - Asymétrique: à clé publique (Merkle-Hellman, RSA, El Gamal)
  - Hybride : clé publique et secrète (PGP)
- Cryptographie : futur et recherche
  - Quantique
  - Courbes elliptiques

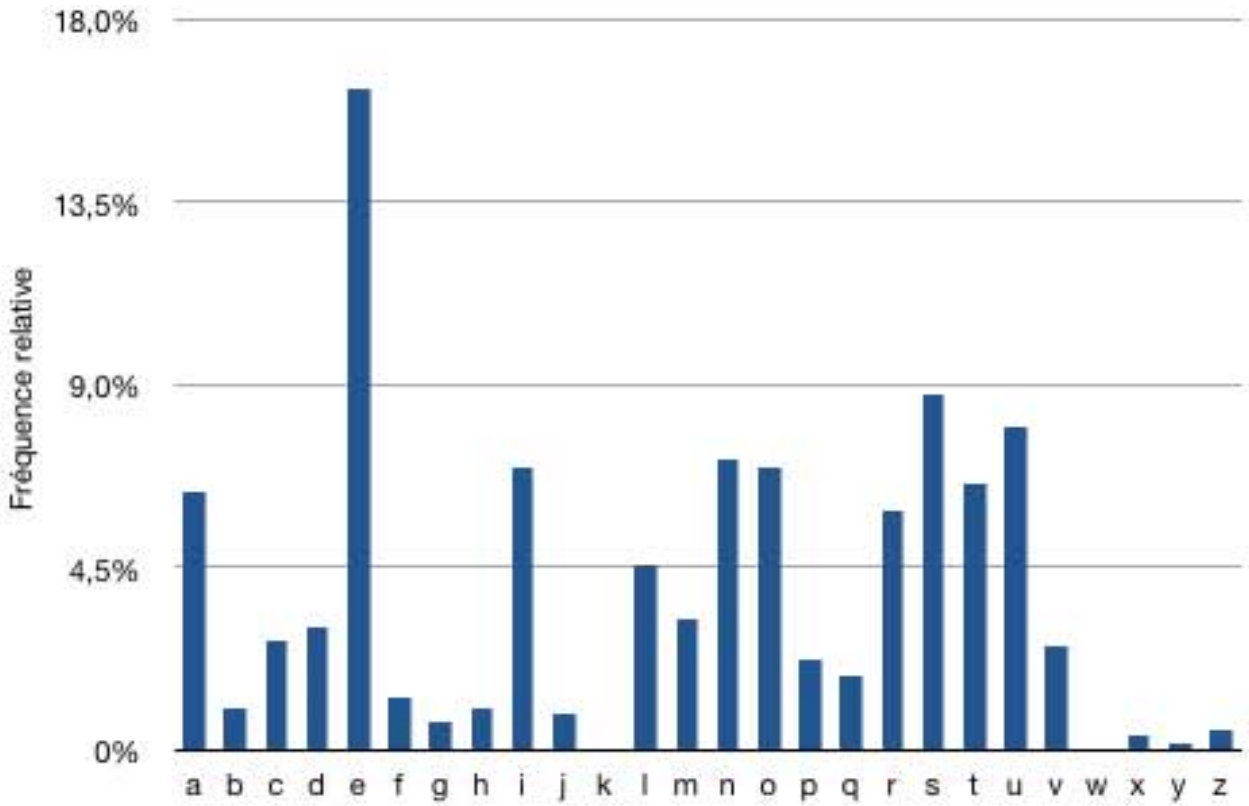
Cryptanalyse

- **Cryptanalyse statistique**.
- **Cryptanalyse différentielle**.
- **Cryptanalyse linéaire**.

Cryptanalyse statistique

- Consiste à mesurer la distribution des fréquences de chaque caractère et à les comparer avec des statistiques similaire
- Le cryptogramme doit être suffisamment long pour avoir des moyennes significatives.
- Chaque langue dispose de fréquences différentes : il faut donc avoir sous les yeux les fréquences de toutes les langues si on ne connaît pas l'origine du message.

Cryptanalyse statistique



Cryptanalyse différentielle

- Étude sur la manière dont les différences entre les données en entrée affectent les différences de leurs sorties.
- Elle s'effectue en général dans un contexte de texte clair choisi.
- La cryptanalyse repose sur des paires de textes clairs qui ont une différence constante.
- L'attaquant calcule ensuite les différences dans les textes chiffrés, afin d'en extraire des motifs pouvant indiquer un biais.
- Les différences en sortie du chiffrement sont nommées des **différentielles**.

Cryptanalyse linéaire

- Établir une équation linéaire entre certains bits du texte en clair et certains du texte chiffré.
- La cryptanalyse linéaire est plus efficace que la cryptanalyse différentielle, mais moins pratique.
- La cryptanalyse linéaire consiste à faire une approximation linéaire de l'algorithme de chiffrement en le simplifiant. En augmentant le nombre de couples disponibles, on améliore la précision de l'approximation et on peut en extraire la clé.

Secret parfait

- Un algorithme de chiffrement assure **le secret parfait** si et seulement si le texte chiffré C ne donne pas d'information supplémentaire sur le texte clair M.

Cryptographie classique

- Les deux techniques de base de la cryptographie classiques de chiffrement sont :
  - **Substitution** : remplacement d'un élément du texte en clair par un élément du texte chiffré.
  - **Transposition** : appelée aussi permutation, modification de l'ordre d'apparence des éléments du texte en clair.

Substitution

- on remplace une lettre par autre chose simple
- Techniques :
  - monoalphabétique.
  - polyalphabétique.

Substitution monoalphabétique

- Une des méthodes de cryptographie les plus anciennes.
- Consiste à remplacer une lettre par une autre.
- Exemples :
  - Alphabets désordonnés
  - Carré de Polybe
  - Chiffre Pig Pen
  - Chiffrement de César (décalage)

Substitution monoalphabétique : Alphabets désordonnés

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

- Exemple :
  - Texte clair : SECURITE
  - Texte chiffré : ?

Substitution monoalphabétique : Alphabets désordonnés

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

- Exemple :
  - Texte clair : SECURITE
  - Texte chiffré : XQUMSRDQ

Substitution monoalphabétique : Carré de Polybe

	1	2	3	4	5
1	a	b	c	d	e
2	f	g	h	i	j
3	k	l	m	n	o
4	p	q	r	s	t
5	u	v	x	y	z

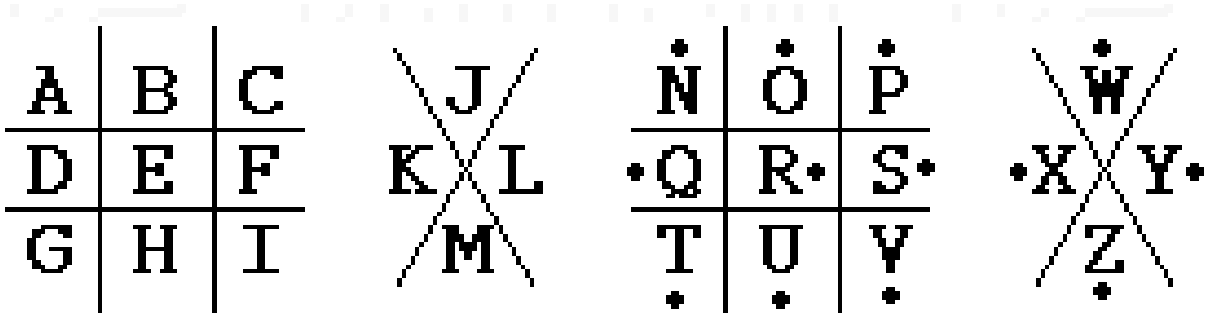
- Exemple :
  - Texte clair : SECURITE
  - Texte chiffré : ?

Substitution monoalphabétique : Carré de Polybe

	1	2	3	4	5
1	a	b	c	d	e
2	f	g	h	i	j
3	k	l	m	n	o
4	p	q	r	s	t
5	u	v	x	y	z

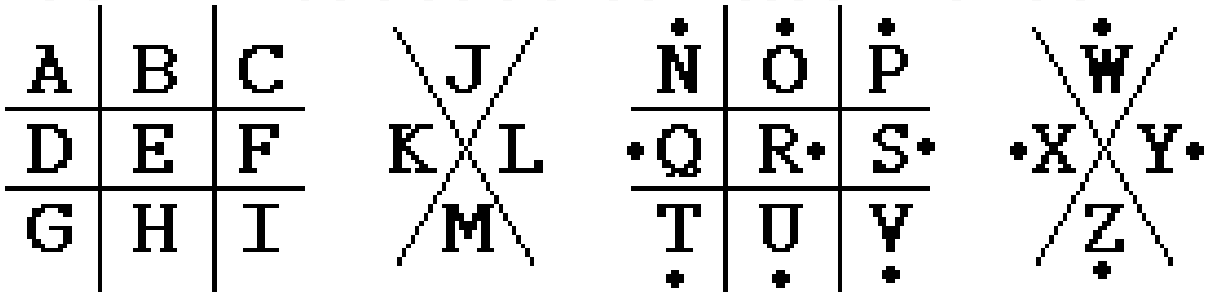
- Exemple :
  - Texte clair : SECURITE
  - Texte chiffré : 4415135143244515

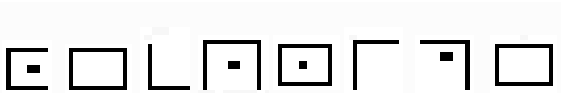
Substitution monoalphabétique : Chiffre Pig Pen



- Exemple :
  - Texte clair : SECURITE
  - Texte chiffré : ?

Substitution monoalphabétique : Chiffre Pig Pen



- Exemple :
  - Texte clair : SECURITE
  - Texte chiffré : 

Substitution monoalphabétique : Chiffrement de César

- Chaque caractère du message en clair est remplacé par un caractère situé à trois positions plus loin dans l'ordre alphabétique
- Si on représente un caractère par sa position dans l'alphabet; la fonction de chiffrement qui consiste à remplacer un caractère m par le caractère c décalé de trois position est :
  - **Chiffrement** : $c = E(m, 3) = (m + 3) \bmod 26$
  - **Déchiffrement** : $m = D(c, 3) = (c - 3) \bmod 26$
  - Avec E : chiffrement, D : déchiffrement

Substitution monoalphabétique : Chiffrement de César

- Exemple :
  - Texte en clair : SECURITE $\rightarrow$ 19 5 3 21 18 9 20 5
  - Texte chiffré : ?

Substitution monoalphabétique : Chiffrement de César

- Exemple :
  - Texte en clair : SECURITE $\rightarrow$ 19 5 3 21 18 9 20 5
  - Texte chiffré : $19 + 3 = 22 \rightarrow$ V

Substitution monoalphabétique : Chiffrement de César

- Exemple :
  - Texte en clair : SECURITE $\rightarrow$ 19 5 3 21 18 9 20 5
  - Texte chiffré : 22 8 6 24 21 12 23 8 $\rightarrow$ VHFXULWH

Substitution monoalphabétique : Chiffrement de César

- Une version plus générale est d'utiliser n'importe quel degré de décalage :
  - **Chiffrement** : $c = E(m, k) = (m + k) \bmod 26$
  - **Déchiffrement** : $m = D(c, k) = (c - k) \bmod 26$
  - Avec k : clé secrète, E : chiffrement, D : déchiffrement

Substitution monoalphabétique : critique

- Consiste en une permutation aléatoire des 26 lettre de l'alphabet.
- La clé secrète est la séquence des lettres de substitution.
- Il existe 26! permutations de l'alphabet $> 4x10^{26}$
- Espace des clés très vaste $\rightarrow$ échec d'une attaque par force brute.
- Mais
  - Si la nature du texte clair est connue $\rightarrow$ peut être cassé facilement par une cryptanalyse statistique.

Substitution polyalphabétique

- Une substitution d'un caractère à la fois $\rightarrow$ trop d'informations sur la structure du texte
- Substituer plusieurs caractères du texte en clair à la fois afin d'altérer la structure du texte
- Consiste à utiliser différents décalages suivant une clé.
- Substituer une lettre du message en clair, par une autre choisie en fonction d'un état du cryptosystème, et non plus de manière fixe comme pour la monosubstitution.
- Exemples :
  - Chiffre de Hill
  - Enigma
  - Chiffre Playfair

Substitution polyalphabétique : Chiffre de Hill

$$\begin{pmatrix} C_k \\ C_{k+1} \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} P_k \\ P_{k+1} \end{pmatrix} \pmod{26} \quad \begin{aligned} C_1 &\equiv aP_1 + bP_2 \pmod{26} \\ C_2 &\equiv cP_1 + dP_2 \pmod{26} \end{aligned}$$

- Exemple :
  - Texte en clair : SECURITE avec $\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$
  - Texte chiffré : ?

Substitution polyalphabétique : Chiffre de Hill

$$\begin{pmatrix} C_k \\ C_{k+1} \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} P_k \\ P_{k+1} \end{pmatrix} \pmod{26}$$

$$C_1 \equiv aP_1 + bP_2 \pmod{26}$$
$$C_2 \equiv cP_1 + dP_2 \pmod{26}$$

- Exemple :
  - Texte en clair : SECURITE avec $\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$
  - Texte chiffré :
    S = 9 * 18 + 4 * 4 mod 26 = 22 → W
    E = 5 * 18 + 7 * 4 mod 26 = 20 → U

Substitution polyalphabétique : Chiffre de Hill

$$\begin{pmatrix} C_k \\ C_{k+1} \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} P_k \\ P_{k+1} \end{pmatrix} \pmod{26} \quad \begin{aligned} C_1 &\equiv aP_1 + bP_2 \pmod{26} \\ C_2 &\equiv cP_1 + dP_2 \pmod{26} \end{aligned}$$

- Exemple :
  - Texte en clair : SECURITE avec $\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$
  - Texte chiffré : WUUUDLFT

Substitution polyalphabétique : Playfair

- Choisir une clé e chiffrement sous la forme d'une chaine de caractère et entrer des lettre de cette clé dans les cellules dune matrice 5 x 5 de gauche vers la droite, le reste des cellules est rempli par les letre restantes dans l'ordre alphabétique
- Exemple : si la clé est INFORMATIQUE

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

Substitution polyalphabétique : Playfair

- Règles :
  - Deux lettre qui font partie de la même ligne de la matrice sont remplacée par les lettres de droite de chaque ligne
  - Deux lettre qui font partie de la même colonne sont replacées par les lettres du dessous
  - Sinon, remplacer chaque lettre du texte en clair dans une paire avec la lettre qui se trouve sur la même ligne mais sur la colonne de l'autre lettre de la paire
  - Si le message est composé de deux fois la même lettre, on insère une nulle (usuellement le X) entre les deux pour éliminer ce doublon.

Substitution polyalphabétique : Playfair

Exemple :

- Texte en clair : chiffrements → CH IF FR EM EN TS
- clé : INFORMATIQUE

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

- Texte chiffré : ?

Substitution polyalphabétique : Playfair

Exemple :

- Texte en clair : chiffrements → CH IF FR EM EN TS
- clé : INFORMATIQUE

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

- Texte chiffré : EL NO OM HE BI UL

Transposition

- Toutes les lettres du messages sont présentes mais dans un ordre différent.
- Il utilise le principe des mathématiques : permutation.

Arrivée de l'informatique

- Machine de Enigma est une machine électromécanique portable servant au chiffrement et au déchiffrement de l'information. Elle fut inventée par l'Allemand Arthur Scherbius, reprenant un brevet du Néerlandais Hugo Koch, datant de 1919. Enigma fut utilisée principalement par les Allemands pendant la Seconde Guerre mondiale.
- Machine de Turing est un modèle abstrait du fonctionnement des appareils mécaniques de calcul, tel un ordinateur et sa mémoire. Ce modèle a été imaginé par Alan Turing en 1936, en vue de donner une définition précise au concept d'algorithme ou de "procédure mécanique".Le travail d'Alan Turing pour décrypter les messages allemands a profondément changé le cours de la seconde guerre mondiale.

Chiffrement symétrique

- Chiffrement à clé secrète ou privée.
- La clé de cryptage et la clé de décryptage sont les mêmes et donc doivent être gardées secrètes.
- Transformations similaires pour codage et décodage (protocoles symétriques).

Chiffrement par bloc symétrique

1. coder l'information source en binaire. On obtient ainsi une chaîne de caractères composée de 0 et de 1.
2. découper cette chaîne en blocs de longueur donnée (par exemple 64 bits ou 128 bits ou 256 bits).
3. chiffrer un bloc en faisant un OU exclusif (ou XOR) bit à bit avec une clé secrète, k, qui est une suite de 0 et de 1 de même longueur, (un XOR est donc l'addition sans retenu en base deux).
4. déplacer et permuter certains bits du bloc.
5. recommencer un certain nombre de fois l'étape précédente, on appelle cela une ronde.
6. passer au bloc suivant et retourner a l'étape 3 jusqu' à ce que tous les blocs soient chiffrés.

Algorithmes de chiffrement symétrique

- DES Data Encryption Standard 1976
- TDES Triple Data Encryption Standard 1990
- IDEA International Data Encryption Algorithm 1991
- Blowfish Coup de poisson 1993
- RC5 Rivest Cipher 1994

Algorithmes de chiffrement symétrique

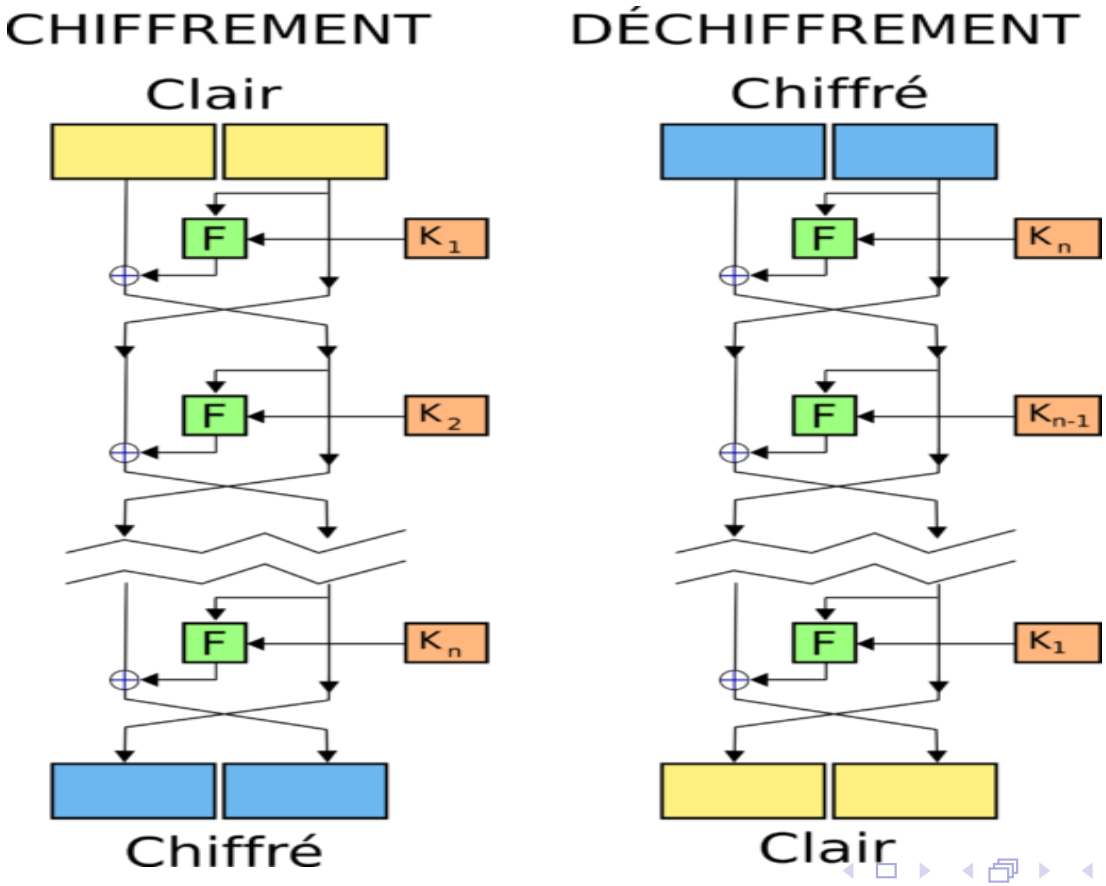
Algorithme de chiffrement par flot		Taille de la clé, commentaires
RC4	Rivest's Cipher / Ron's Code	Taille de clé variable

Algorithme de chiffrement par blocs		Taille de la clé, commentaires
RC5	Rivest's Cipher / Ron's Code	Breveté par RSA Data Security, Chiffrement par blocs, clé variable (jusqu'à 2024 bits)
DES	Data Encryption Standard	Blocs de 64 bits, Clé de 56 bits, 16 tours
TripleDES	Triple Data Encryption Standard	Blocs de 64 bits, Clé de 168 bits mais 112 bits effectifs, 3 fois x 16 tours de DES
IDEA	International Data Encryption Standard	Blocs de 64 bits, clé de 128 bits, 8 tours
AES	Advanced Encryption Standard	Blocs de 128 bits, Clé de 128, 192 ou 256 bits, 10, 12 ou 14 tours selon la taille de la clé

Réseaux Feistel

- La plupart des algorithmes de chiffrement par blocs utilisés actuellement dans le monde civil sont des réseaux de Feistel.
- Dans ce système de chiffrement, un bloc de texte en clair est découpé en deux ; la transformation de ronde est appliquée à une des deux moitiés, et le résultat est combiné avec l'autre moitié par OU exclusif. Les deux moitiés sont alors inversées pour l'application de la ronde suivante.

Réseaux Feistel



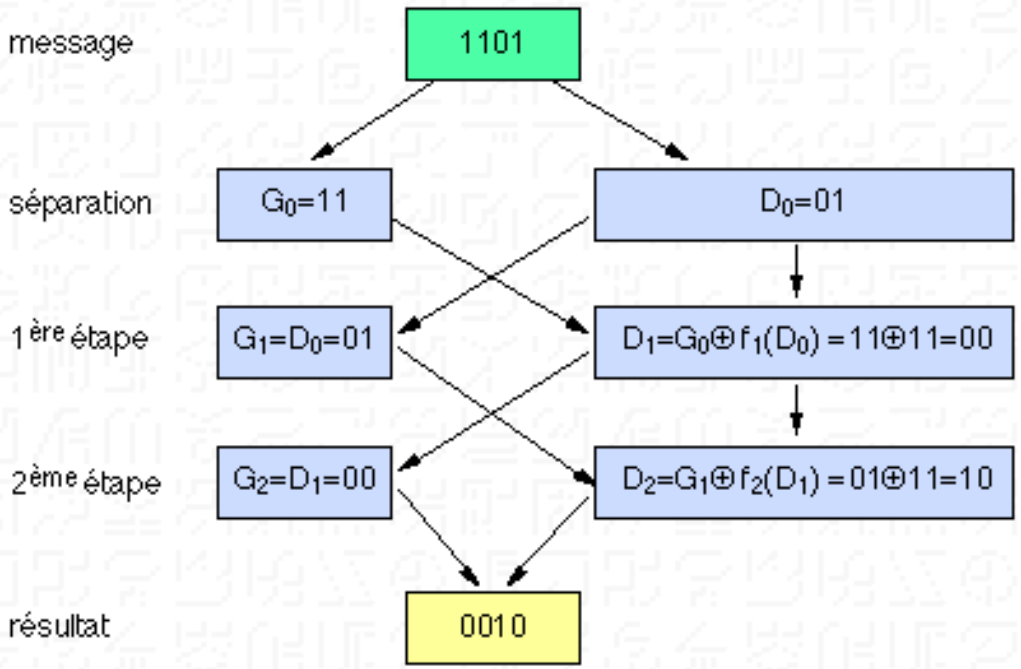
Réseaux Feistel : Exemple

À titre d'exemple, nous allons chiffrer par un réseau de Feistel à deux rondes un message constitué de quatre bits ($24 = 16$ possibilités de messages), ce qui revient à construire une bijection de quatre bits vers quatre bits à partir de deux fonctions f1 et f2 de deux bits vers deux bits.
Nous considérerons que pour une certaine clef entrée, ces fonctions sont les suivantes:

entrée	f_1	sortie
00	→	01
01	→	11
10	→	10
11	→	01

entrée	f_2	sortie
00	→	11
01	→	00
10	→	00
11	→	01

Réseaux Feistel : Exemple



message	résultat
0000	0100
0001	1100
0010	1010
0011	0111
0100	0011
0101	1001
0110	1111
0111	0000
1000	1101
1001	0101
1010	0001
1011	1110
1100	1000
1101	0010
1110	0110
1111	1011

Avantages et inconvénients

- Avantage. Algorithmes en général très rapides
- Inconvénient. Il faut pouvoir échanger la clé !

Chiffrement asymétrique

- Le principe de chiffrement asymétrique (appelé aussi chiffrement à clés publiques) est apparu en 1976.
- 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.
- Les utilisateurs s'échangent cette clé publique au travers d'un canal non sécurisé.

Chiffrement par bloc asymétrique

1. coder l'information source en binaire. On obtient ainsi une chaîne de caractères composée de 0 et de 1.
2. découper cette chaîne en blocs de longueur donnée (par exemple 1024 bits à 2048 bits pour RSA et El Gamal, 256 bits pour les codes elliptiques (des échanges de clés sur un canal non- sécurisé ou un chiffrement asymétrique)).
3. chiffrer un bloc en utilisant la fonction de chiffrement (exponentiation modulaire pour RSA).
4. passer au bloc suivant et retourner à l'étape 3 jusqu'à ce que tous les blocs soient chiffrés.

Algorithmes de chiffrement asymétrique

- RSA : est algorithme décrit en 1977 par Ronald Rivest, Adi Shamir et Leonard Adleman (le plus utilisé).
- Cryptosystème de ElGamal : est un algorithme créé par Taher Elgamal en 1984.
- Cryptosystème de Merkle-Hellman: est un algorithme, défini par Ralph Merkle et Martin Hellman en 1978.

RSA

- Rivest Shamir Adleman ou RSA est un algorithme asymétrique de cryptographie à clé publique,
  - très utilisé dans le commerce électronique,
  - et plus généralement pour échanger des données confidentielles sur Internet.
- Cet algorithme a été décrit en 1977 par Ron Rivest, Adi Shamir et Len Adleman, d'où le sigle RSA.
- Les clefs RSA sont habituellement de longueur comprise entre 1024 et 2048 bits.

RSA

- Principe :
  - Il est facile de fabriquer de grands nombres premiers p et q (>100)
  - Étant donné un nombre entier n = pq, il est très difficile de retrouver les facteurs p et q

RSA

- Création des clés :
  - La clé secrète : 2 grands nombres premiers **p** et **q**
  - La clé publique : **n** = pq ; un entier **e** premier avec (p-1)(q-1)
- Chiffrement :
  - Le chiffrement d'un message M en un message codé C se fait suivant la transformation suivante :
  - $C = M^e \ mod \ n$
- Déchiffrement :
  - il s'agit de calculer la fonction réciproque
  - $M = C^d mod \ n$
  - Avec : $e * d \ mod \ ((p-1)(q-1)) = 1$

RSA

- Remarques :
  - On transforme d'abord les lettres du message en nombres et ceci en remplaçant chaque lettre par son rang dans l'alphabet.
  - On découpe ensuite le message chiffré en blocs de même longueur mais plus petit que n.

RSA : Exemple

- Chiffrer le message INFORMATIQUE avec RSA en utilisant la paire de clé secrète (p, q) = (11, 13).
- Solution : ?

RSA : Exemple

- Chiffrer le message INFORMATIQUE avec RSA en utilisant la paire de clé secrète (p, q) = (11, 13).
- Solution :
  - Calculer la valeur de la paire de clé publique (n, e) :
    - $n = p * q = 11 * 13 = 143$
    - e est premier avec (p - 1)*(q - 1) = 10 * 12 = 120 $\rightarrow$ e = 7, 11, 13, ...
    - (n, e) = (143, 7)

RSA : Exemple

- Chiffrer le message INFORMATIQUE avec RSA en utilisant la paire de clé secrète (p, q) = (11, 13).
- Solution :
  - Calculer la valeur de la paire de clé publique (n, e) = (143, 7)
  - Convertir les lettres en chiffres et les regrouper en bloc :
    - INFORMATIQUE = 09 14 06 15 18 13 01 20 09 17 21 05
    - Taille des blocs : 3
    - Blocs : 091 406 151 813 012 009 172 105

RSA : Exemple

- Chiffrer le message INFORMATIQUE avec RSA en utilisant la paire de clé secrète (p, q) = (11, 13).
- Solution :
  - Calculer la valeur de la paire de clé publique (n, e) = (143, 7)
  - Convertir les lettres en chiffres et les regrouper en bloc : 091 406 151 813 012 009 172 105
  - Chiffrer les blocs du message :
    - $C = M^e \ mod \ n$
    - $C_1 = 091^7 \ mod \ 143 = 130$
    - $C_2 = 406^7 \ mod \ 143 = 120$
    - ....
    - Blocs chiffrés = 130 120 057 032 012 048 094 118

RSA : Exemple

- Chiffrer le message INFORMATIQUE avec RSA en utilisant la paire de clé secrète (p, q) = (11, 13).
- Solution :
  - Calculer la valeur de la paire de clé publique (n, e) = (143, 7)
  - Convertir les lettres en chiffres et les regrouper en bloc : 009 140 615 181 301 200 917
  - Chiffrer les blocs du message : 130 120 057 032 012 048 094 118
  - On peut reconvertir les nombres en chiffres pour obtenir le message chiffré :
    - désassembler les blocs de : 13 01 20 05 70 32 01 20 48 09 41 18
    - On utilise le modulo 26 pour les nombres $> 26 \rightarrow$ 13 01 20 05 18 06 01 20 22 09 15 18
    - Texte chiffré = MATERFATVIOR

RSA : Exemple

- Chiffrer le message INFORMATIQUE avec RSA en utilisant la paire de clé secrète (p, q) = (11, 13).
- Solution :
  - Calculer la valeur de la paire de clé publique (n, e) = (143, 7)
  - Convertir les lettres en chiffres et les regrouper en bloc : 009 140 615 181 301 200 917
  - Chiffrer les blocs du message : 130 120 057 032 012 048 094 118
  - On peut reconvertir les nombres en chiffres pour obtenir le message chiffré : MATERFATVIOR

Avantages et Inconvénients

- Le problème consistant à se communiquer la clé de déchiffrement n'existe plus, dans la mesure où les clés publiques peuvent être envoyées librement.
- Le chiffrement par clés publiques permet donc à des personnes d'échanger des messages chiffrés sans pour autant posséder de secret en commun.
- En contrepartie, tout le challenge consiste à s'assurer que la clé publique que l'on récupère est bien celle de la personne à qui l'on souhaite faire parvenir l'information chiffrée !

Fonction de Hachage

- Une fonction de hachage (parfois appelée fonction de condensation) est une fonction permettant d'obtenir un condensé (appelé aussi **condensat** ou **haché** ou en anglais message **digest**) d'un texte,
- C'est une suite de caractères assez courte représentant le texte qu'il condense (**résumé**).
- une chaîne de caractères de taille fixe, qui s'étend le plus souvent sur **128, 160, 256,** voir **512 bits**.
- Ainsi, le haché représente en quelque sorte **l'empreinte digitale** (en anglais **finger print**) du document.

Fonction de Hachage

- Sur Internet, on part du principe qu'une empreinte numérique correspond à un document unique.
- Une modification à l'intérieur d'un document, même atomique, provoque un changement radical de son empreinte.
- Les fonctions de hachage sont des fonctions à sens unique: il est aisé de calculer l'empreinte numérique d'un document, mais il est très difficile de retrouver le document initial à partir de son empreinte.

Algorithmes de Hachage : MD5

- MD (Message Digest).
- Versions : MD — MD2 — MD4 — MD5
- 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.

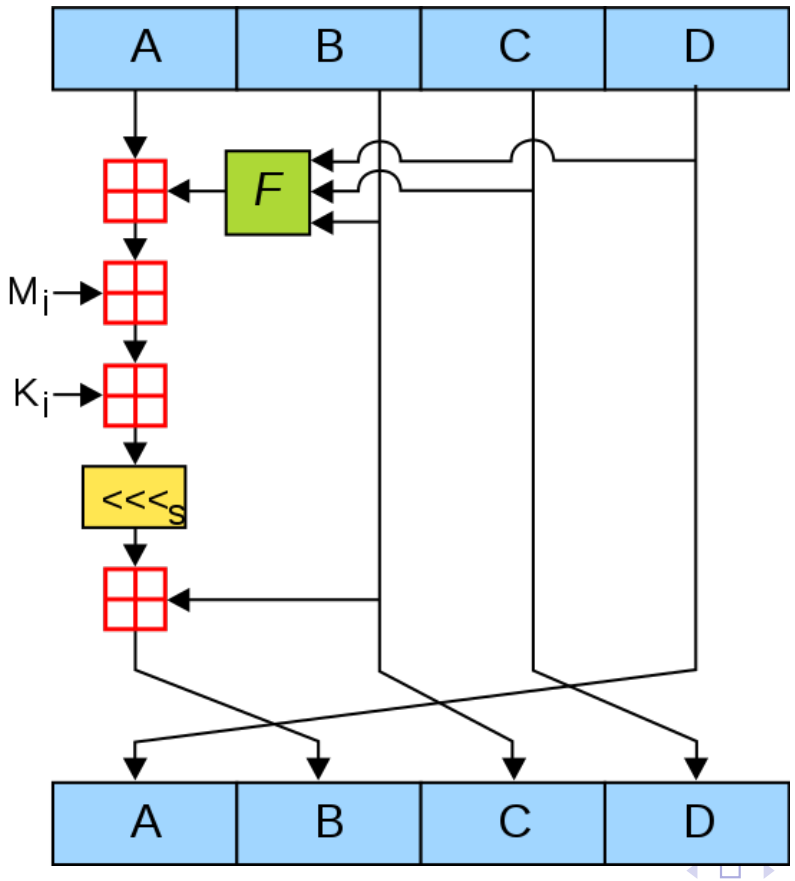
Algorithmes de Hachage : MD5 - Algorithme

- On travaille itérativement sur des blocs de 512 bits.
- On définit 4 buffers de 32 bits A,B,C et D, initialisés ainsi : 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))

Algorithmes de Hachage : MD5 - Algorithme

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

Algorithmes de Hachage : MD5 - Algorithme



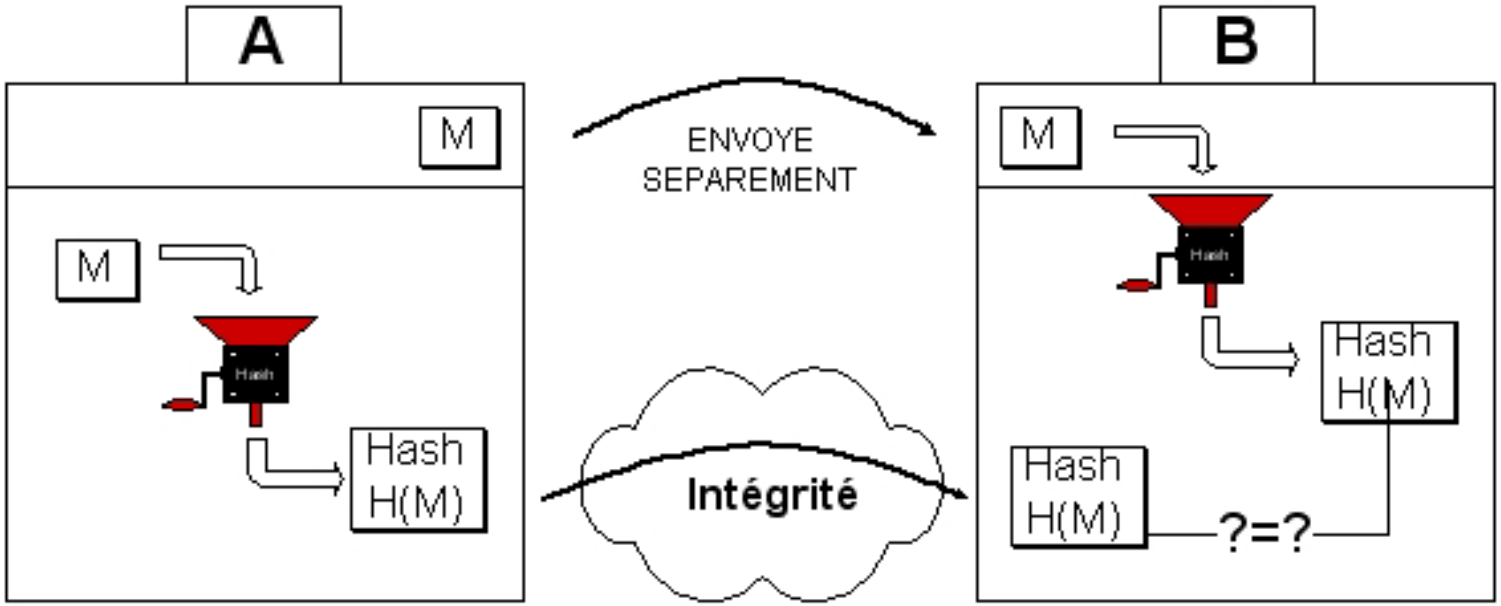
Algorithmes de Hachage : SHA

- SHA (Secure Hash Algorithm), pouvant être traduit par Algorithme de hachage sécurisé;
- Versions : SHA-0, SHA-1, SHA-224, SHA-256, SHA-384, SHA-512.
- SHA-1 : crée des empreintes d'une longueur de **160 bits** à partir d'un message en le traitant par blocs de 512 bits.

Intégrité

- En expédiant un message accompagné de son haché, il est possible de garantir l'**intégrité** d'un message.
- Le destinataire peut vérifier que le message n'a pas été altéré (**intentionnellement** ou de manière **accidentelle**) durant la communication.
- Lors de la réception du message, il suffit au destinataire de **calculer le haché** du message reçu et de le comparer avec le haché accompagnant le document.
- Si le message (ou le haché) a été falsifié durant la communication, les deux empreintes ne correspondront pas.

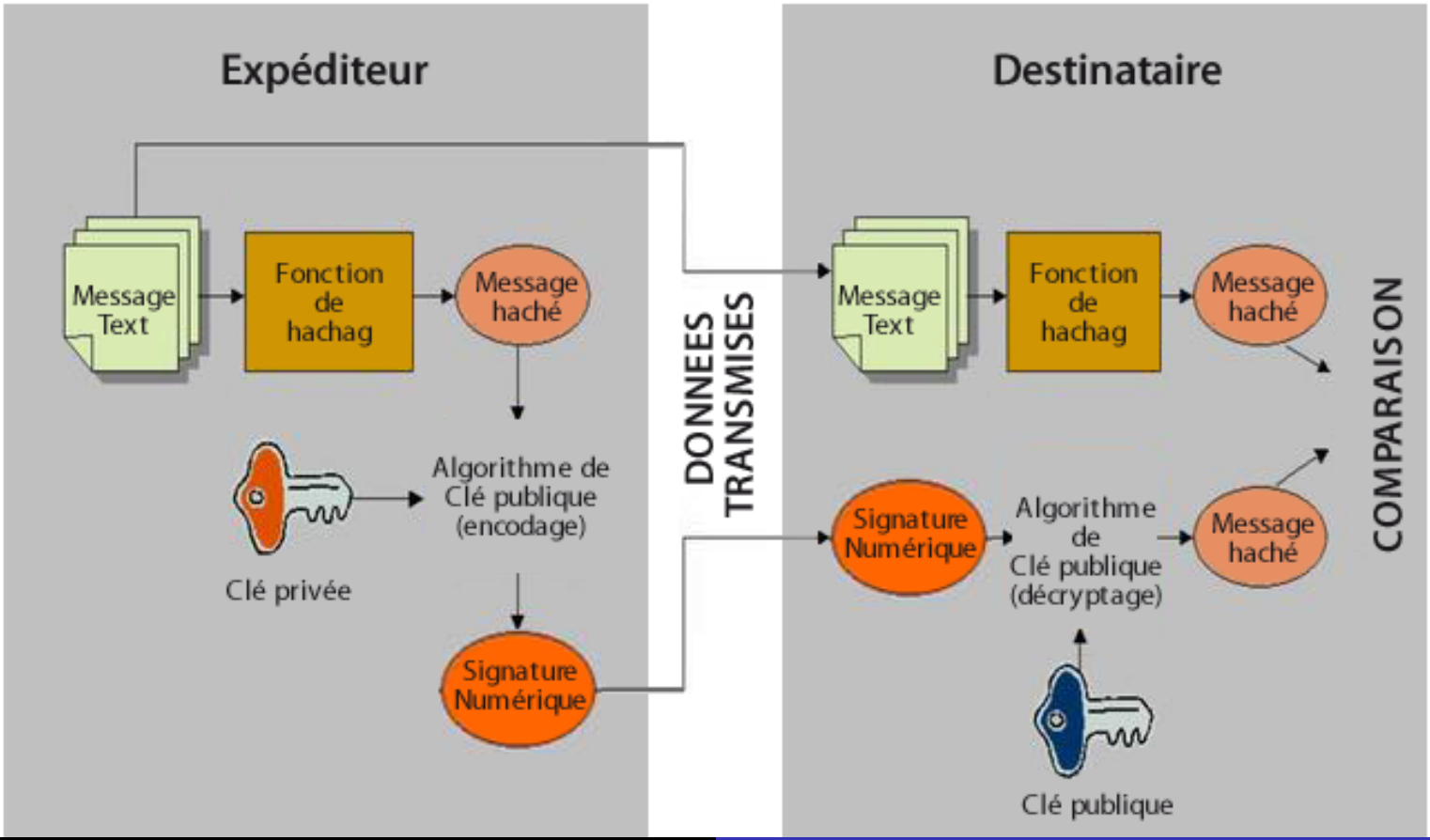
Intégrité


A
M
M
Hash
Hash
H(M)
ENVOYE
SEPAREMENT
Intégrité
B
M
Hash
Hash
H(M)
Hash
H(M)
?=?

Authentification du message

- L'utilisation d'une fonction de hachage permet de vérifier que l'empreinte correspond bien au message reçu, mais rien ne prouve que le message a bien été envoyé par celui que l'on croit être l'expéditeur.
- Pour garantir l'authentification du message, il suffit à l'expéditeur de chiffrer (signer) le condensé à l'aide de sa clé privée (le haché signé est appelé **signature**) et d'envoyer la signature au destinataire.
- A réception du message, il suffit au destinataire de déchiffrer la signature avec la clé publique de l'expéditeur, puis de **comparer le haché obtenu avec la fonction de hachage au haché reçu** en pièce jointe.

Signature numérique



Signature numérique : Algorithme

- Calcul de l'empreinte des données à signer.
- Chiffrement de l'empreinte à l'aide de la clé privée. On obtient alors la signature.
- Déchiffrement de la signature avec la clé publique. Cela permet de retrouver l'empreinte associée aux données signées.
- Calcul de l'empreinte des données signées. On vérifie que cette empreinte correspond à la précédente, auquel cas la signature est valide : les données sont donc intègres et l'identité de l'expéditeur est vérifiée.

Signature numérique

La signature numérique permet de :

- Vérifier l'intégrité du message.
- Identifier et garantir l'authenticité (l'identité) du expéditeur.
- Assurer la non-répudiation (assurer que l'expéditeur a bien envoyé le message).

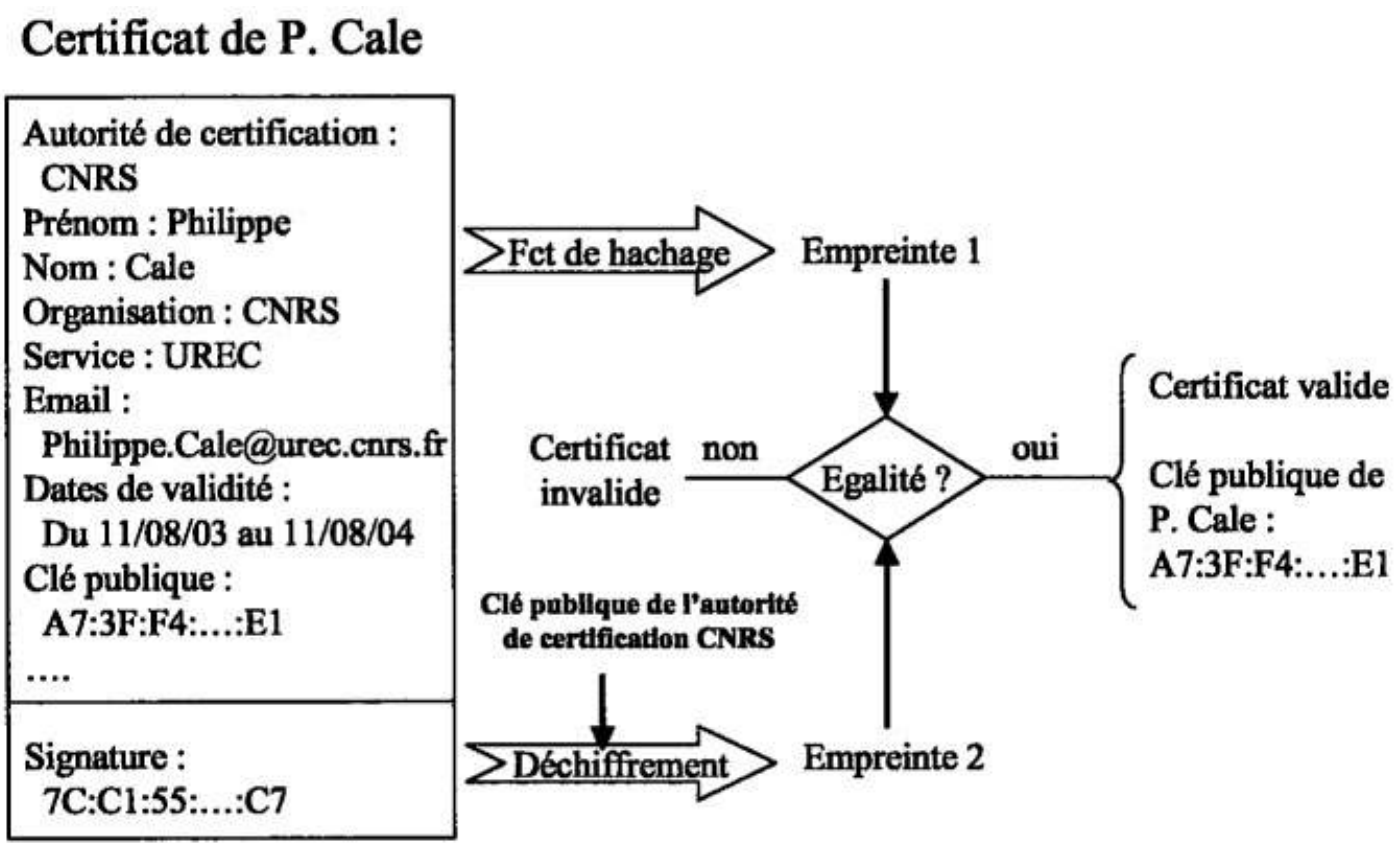
Certificat numérique

- Le partage de la clé publique du chiffrement asymétrique se fait à travers un annuaire électronique (généralement au format LDAP- Lightweight Directory Access Protocol) ou bien d'un site web.
- Un certificat permet d'associer une clé publique à une entité (une personne, une machine, un serveur) 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 (souvent notée CA pour Certification Authority).

Certificat numérique

- Le partage de la clé publique du chiffrement asymétrique se fait à travers un annuaire électronique (généralement au format LDAP- Lightweight Directory Access Protocol) ou bien d'un site web.
- Un certificat permet d'associer une clé publique à une entité (une personne, une machine, un serveur) 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 (souvent notée CA pour Certification Authority).

Certificat numérique



Cryptographie quantique

- Secret parfait $\rightarrow$ problème de partage de la clé.
- Se base sur les mathématiques et **physiques** (l'incertitude d'Heisenberg).
- Dans le transport de clé "quantique", l'information est transportée par des **photons**.

Cryptographie quantique : Photons

- Photons
  - les plus petites entités physiques de la vie.
  - des particules élémentaires de lumière (énergie) au niveau quantum.
- Chaque photon peut être polarisé, c'est-à-dire que l'on impose une direction à son champ électrique. La polarisation est mesurée par un angle qui varie de 0° à 180°.
- La polarisation peut prendre 4 valeurs : 0° (↔), 45° (↗), 90° (↕), 135° (↖).

Cryptographie quantique : Détection de polarisation

- Pour détecter la polarisation des photons, on utilise un **filtre polarisant** suivi d'un **détecteur de photons**.
- Si un photon polarisé à 0° rencontre un filtre polarisant orienté à 0°, il traverse ce filtre et est enregistré par le détecteur ($\leftrightarrow$ est enregistré comme $\leftrightarrow$).
- Si un photon polarisé à 90° rencontre le même filtre, il est stoppé et le détecteur n'enregistre rien ($\updownarrow$ n'est pas enregistré).
- Si un photon est polarisé diagonalement (45° ou 135°), une fois sur deux, il traverse le filtre, et une fois sur deux, il est stoppé. ($\nearrow$ ou $\nwarrow$ est soit enregistré soit non).

Cryptographie quantique : Détection de polarisation

- Avec un filtre polarisant orienté à 0° :
  - On peut distinguer entre une polarisation à 0° et à 90°.
  - Il est impossible de distinguer en même temps entre une polarisation à 45° et à 135°.
- De la même façon, on peut utiliser un filtre polarisant orienté à 45° : il laisse passer les photons polarisés à 45°, stoppe ceux polarisés à 135°, et se comporte aléatoirement avec ceux à 0° et 90°

Cryptographie quantique : Algorithme d'échanges de clé

- L'émetteur envoie au récepteur une clé secrète constituée de 0 et de 1.
- Les photons polarisés à 0° ou 45° représentent 0, et ceux polarisés à 90° ou 135° représentent 1.
- L'émetteur envoie sur un canal quantique, une suite de photons polarisés au hasard parmi 0°, 45°, 90° et 135°.
- A l'autre bout, le récepteur reçoit les photons et mesure aléatoirement leur polarisation **rectiligne** (filtre placé à 0°), ou leur polarisation **diagonale** (filtre placé à 45°). Si le photon traverse le filtre, le récepteur note 0, sinon il note 1.
- Certaines mesures du récepteur (en moyenne, une sur deux) n'ont pas d'intérêt.
- La clé secrète représente les mesures correctes après vérification du filtre avec l'émetteur.

Cryptographie quantique : Exemples

- Bits à émettre : 0 0 1 1 1 0 0 1
- Photons émis : ↗ ↔ ↕ ↕ ↘ ↗ ↔ ↕
- Filtre utilisé : 45° 45° 0° 0° 0° 0° 0° 45°
- Photon passe? oui non non non non oui oui oui
- Valeur en bits : 0 1 1 1 1 0 0 0
- Correction filtre: V F V V F F V F
- Clé secrète : 0 1 1 0

Cryptographie quantique

- La cryptographie quantique a dépassée la phase de recherche $\rightarrow$ Développement et commercialisation.
- Limite : vitesse et distance (200KM).

Courbes elliptiques

- Proposée par Victor Miller et Neal Koblitz en 1985.
- Elles permettent de remplacer les calculs sur des entiers, par des calculs dans les groupes associés à une courbe elliptique.
- Une courbe elliptiques a la forme suivante:
  $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$
- En cryptographie, a_1, a_2 et a_3 doivent être égaux à 0.
- En renommant $a_4 = a$ et $a_6 = b$, on obtient :
  $y^2 = x^3 + ax + b$

Courbes elliptiques : Échanges de clés

- L'émetteur et le récepteur choisissent ensemble une courbe elliptique E(a,b,K) et un point P sur la courbe. Cet échange n'a pas besoin d'être sécurisé.
- L'émetteur choisit secrètement k_A et envoie $k_A * P$ au récepteur. Cet échange n'a pas besoin d'être sécurisé.
- En même temps, le récepteur choisit secrètement k_B et envoie $k_B * P$ à l'émetteur. Cet échange n'a pas besoin d'être sécurisé.
- L'émetteur calcule $k_A * (k_B * P) = (k_A * k_B) * P$.
- Le récepteur calcule $k_B * (k_A * P) = (k_A * k_B) * P$.

Courbes elliptiques : Sécurité

- Si un attaquant a récupéré l'échanges, il connait E(a,b,K), P, $k_A P$ et $k_b P$.
- Pour pouvoir retrouver la clé $k_A * k_B * P$ il faut pouvoir calculer k_A connaissant P et $k_A * P \rightarrow$ consiste à résoudre le logarithme discret sur la courbe elliptique.
- C'est le même type de problème, avec des notations additives, que de retrouver n dans une équation $y \equiv xn[p]$, avec x,y et p connus $\rightarrow$ Problème très difficile.

Courbes elliptiques : Avantages et Inconvénients

- Avantages :
  - Pour craquer la clé, il faut résoudre le logarithme discret sur le groupe de la courbe elliptique $\rightarrow$ Ces groupes sont plus difficiles à manipuler, ils peuvent différer beaucoup les uns des autres si on change les paramètres.
  - Une clé de 200 bits pour les chiffres basés sur les courbes elliptiques est plus sûre qu'une clé de 1024 bits pour le RSA.
  - Les calculs sur les courbes elliptiques ne sont pas compliqués à réaliser.

Courbes elliptiques : Avantages et Inconvénients

- Inconvénients :
  - La théorie des fonctions elliptiques est complexe, et récente. Il n'est pas exclu que des trappes permettent de contourner le problème du logarithme discret.
  - La technologie de cryptographie par courbe elliptique a fait l'objet du dépôt de nombreux brevets à travers le monde $\rightarrow$ utilisation très coûteuse.

Questions?