LA CRYPTOGRAPHIE

Introduction et définitions

- Depuis l'Egypte ancienne, l'homme a voulu pouvoir échanger des informations de façon **confidentielle.**
- Il existe de nombreux domaines où ce besoin est vital :
- militaire
- commercial
- bancaire
- de la vie privée
- diplomatique

Définitions

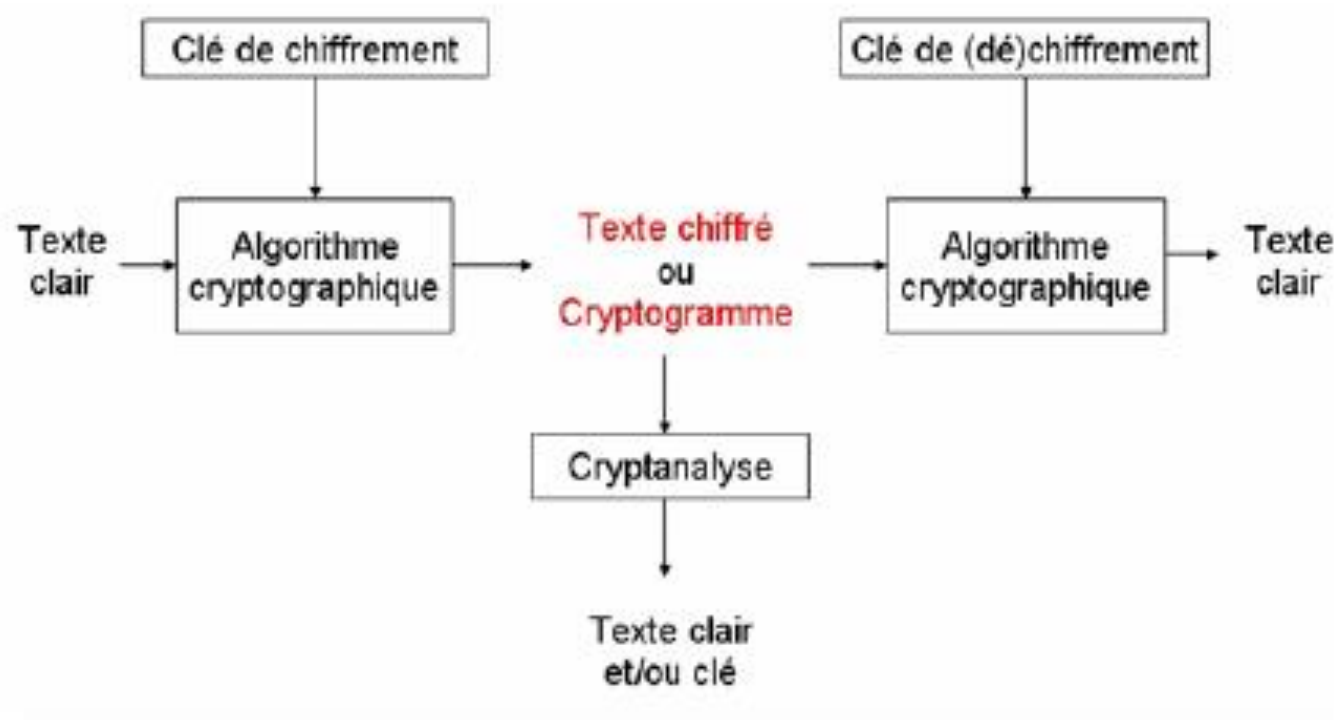
- En grec :

Cryptographie : (κρυπτο . γραf ην)

écriture cachée / brouillée.

- Pour assurer la protection des accès à une information, on utilise des techniques de **chiffrement.**
- Le **chiffrement** consiste à transformer une donnée (texte, message, ...) afin de la rendre incompréhensible par une personne autre que celui qui a créé le message et celui qui en est le destinataire. La fonction permettant de retrouver le texte clair à partir du texte chiffré porte le nom de **déchiffrement**.

Quelques notions



Quelques notions

- **Cryptologie :** Il s'agit d'une science mathématique comportant deux branches : la cryptographie et la cryptanalyse
- **Cryptographie :** La cryptographie est l'étude des méthodes donnant la possibilité d'envoyer des données de manière confidentielle sur un support donné.
- **Texte chiffré :** Appelé également **cryptogramme**, le texte chiffré est le résultat de l'application d'un chiffrement à un texte clair.
- **Cryptanalyse** : Opposée à la cryptographie, elle a pour but de retrouver le texte clair à partir de textes chiffrés en déterminant les failles des algorithmes utilisés.
- **Cryptosystème** : Il est défini comme l'ensemble des clés possibles (espace de clés), des textes clairs et chiffrés possibles associés à un algorithme donné.

Les méthodes se décomposent en deux grandes familles de chiffrement :

- par **substitution ;**
- par **transposition.**

Chiffrement par substitution

- **mono-alphabétique (code César)** consiste à remplacer chaque lettre du message par une autre lettre de l'alphabet ;
- **Poly-alphabétique (code Vigenère)** consiste à utiliser une suite de chiffrement, mono-alphabétique réutilisée périodiquement ;
- **poly-grammes (Hill)** consiste à substituer un groupe de caractères (poly-gramme) dans le message par un autre groupe de caractères.

Chiffrement de César

$C = E(p) = (p + k) \bmod 26$

p est l'indice de la lettre de l'alphabet, k est le décalage.

Alphabet clair : abcdefghijklmnopqrstuvwxyz

Alphabet chiffré : DEFGHIJKLMNOPQRSTUVWXYZABC

Texte clair :

errare humanum est, perseverare diabolicum

Texte chiffré :

HUUDUH KXPDQXP HVW, SHUVHYHUDUH GLDEROLFXP

Le chiffre de Vigenère

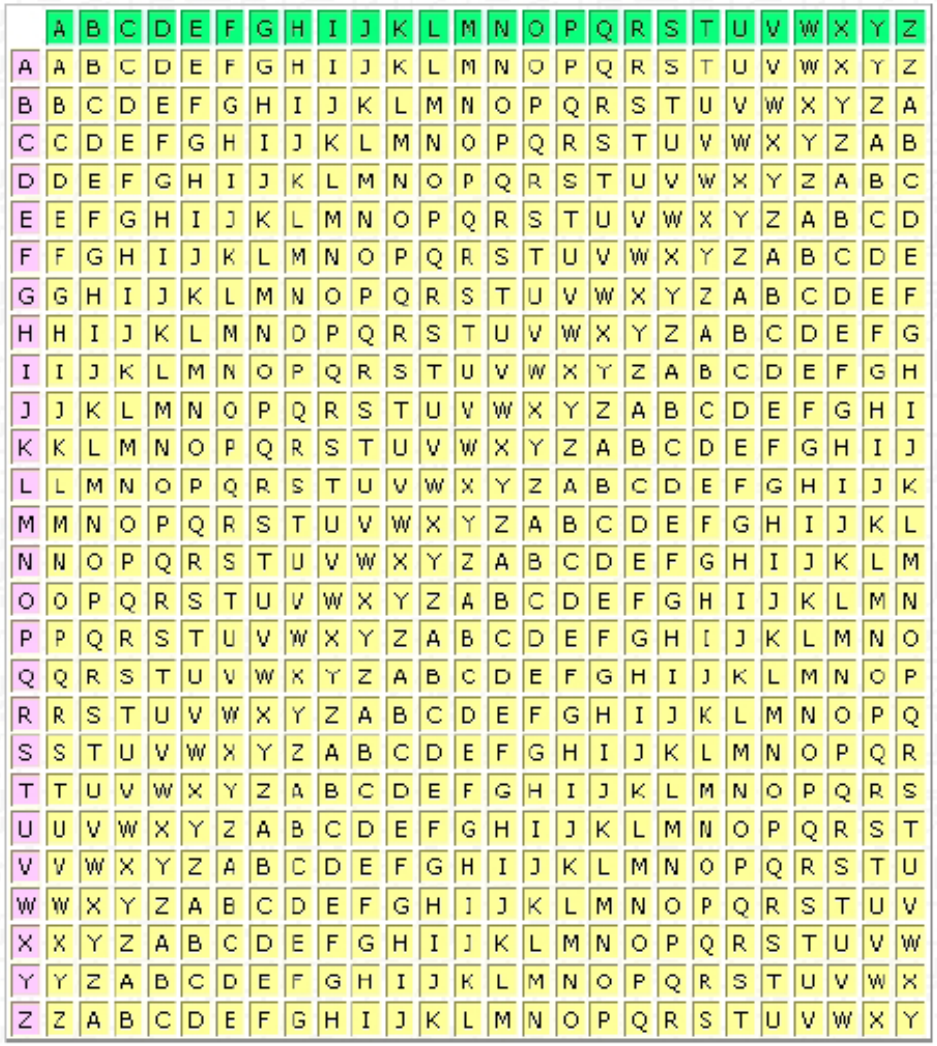
- Ce chiffre utilise une clef qui définit le décalage pour chaque lettre du message (A : décalage de 0 cran, B : 1 cran, C : 2 crans, ..., Z : 25 crans).
- Exemple : chiffrer le texte "CHIFFRE DE VIGENERE" avec la clef "BACHELIER" (cette clef est éventuellement répétée plusieurs fois pour être aussi longue que le texte clair)

Clair	C	H	I	F	F	R	E	D	E	V	I	G	E	N	E	R	E
Clef	B	A	C	H	E	L	I	E	R	B	A	C	H	E	L	I	E
Décalage	1	0	2	7	4	11	8	4	17	1	0	2	7	4	11	8	4
Chiffré	D	H	K	M	J	C	M	H	V	W	I	I	L	R	P	Z	I

Le chiffre de Vigenère

- Pour utiliser le chiffrement de Vigenère, on a recours au Carré de Vigenère La lettre de la clef est dans la colonne la plus à gauche, la lettre du message clair est dans la ligne tout en haut. La lettre chiffrée est à l'intersection des deux.

Le carré de Vigenère



	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

Chiffre de Hill

Les lettres sont d'abord remplacées par leur rang dans l'alphabet. Les lettres P_k et P_{k+1} deviennent C_k et C_{k+1}

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

Les composantes de cette matrice doivent être des entiers positifs. De plus la matrice doit être inversible dans Z_{26}. Cependant, sa taille n'est pas fixée à 2. Elle grandira selon le nombre de lettres à chiffrer simultanément.

Chiffrement par transposition

Toutes les lettres du message sont présentes, mais dans un ordre différent.

C'est un chiffrement de type *anagramme*. Il utilise le principe mathématique des **permutations (par colonne par exemple).**

En général : **réarranger géométriquement les données pour les rendre visuellement inexploitables.**

Par exemple : « Ceci est un texte à chiffrer de la plus haute importance »

Le texte est regroupé en tableau, suivant un nombre de colonnes donné.

Chaque colonne est ensuite copiée l'une après l'autre.

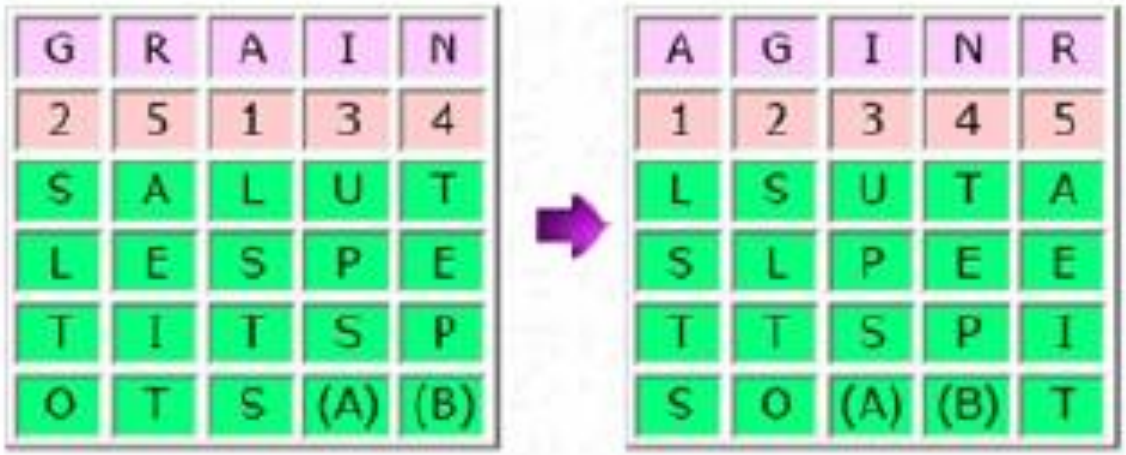
```
Ceci est u
n texte à
chiffrer d
e la plus
haute impo
rtance
```

Cncehre h atctiluaiefatn…

Transposition avec clé

on a choisi comme clef GRAIN pour chiffrer le message SALUT LES PETITS POTS. En remplissant la grille, on constate qu'il reste deux cases vides, que l'on peut remplir avec des nulles

(ou pas, selon les désirs des correspondants).

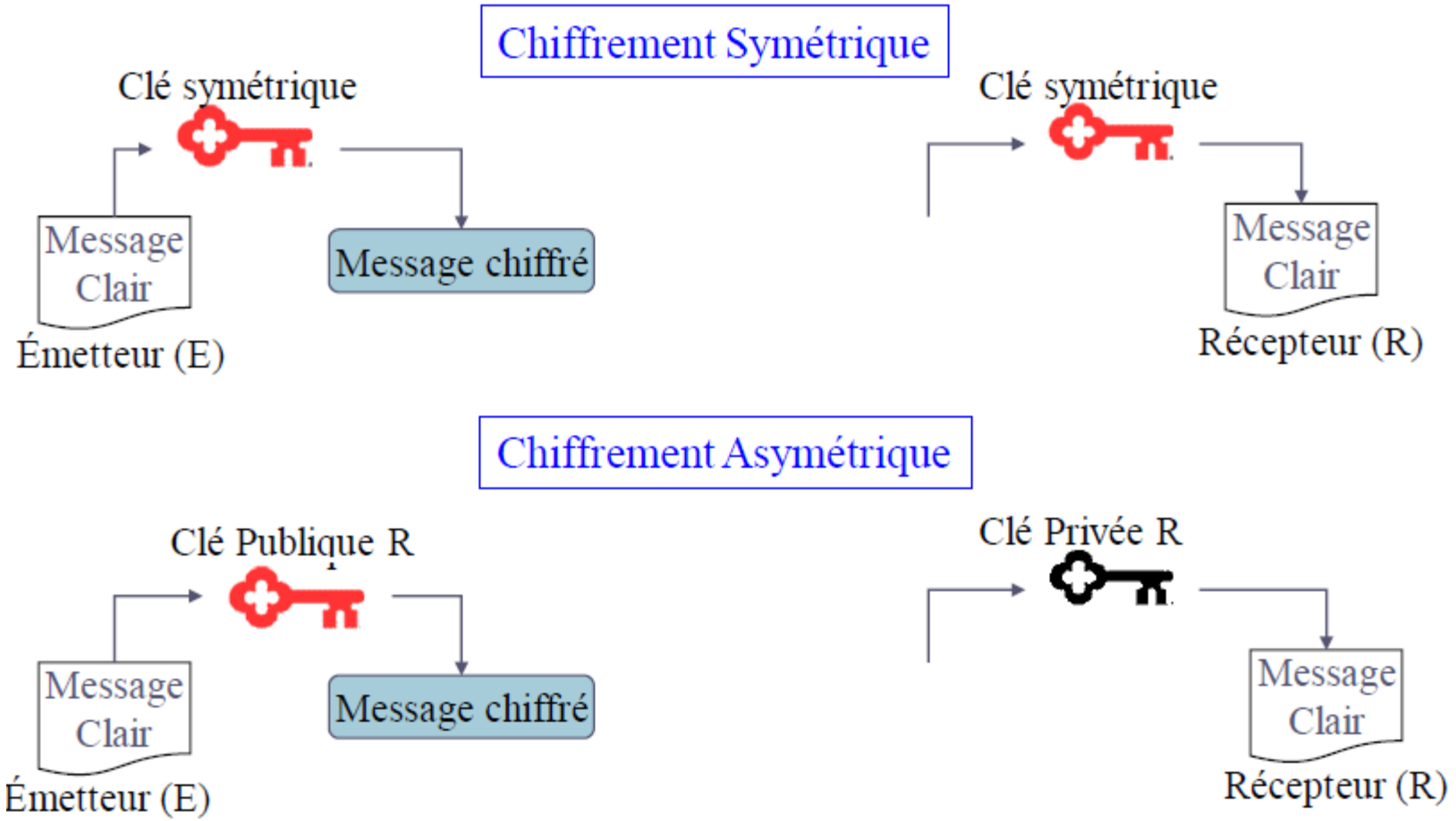


Cryptographie moderne

Clé de chiffrement

- Dans la cryptographie moderne, l'habilité de maintenir un message chiffré secret, repose non pas sur l'algorithme de chiffrement (qui est largement connu), mais sur une information secrète dite **CLE** qui doit être utilisée avec l'algorithme pour produire le message chiffré.
- Selon que la clé utilisée pour le chiffrement et le déchiffrement est la même ou pas, on parle de système cryptographique **symétrique** ou **asymétrique.**

Chiffrement symétrique vs. Chiffrement asymétrique



Algorithmes de chiffrement symétrique

Chiffrement par bloc : division du texte clair en blocs fixe, puis chiffrement bloc par bloc

- DES: IBM, Standard NIST 1976
- 3DES: W. Diffie, M. Hellman, W. Tuchmann 1978.
- IDEA: Xuejia Lai et James Massey en 1992
- Blowfish: Bruce Schneier en 1993
- AES (Rijndael): Joan Daemen et Vincent Rijmen 2000

Chiffrement par flux : le bloc a une dimension unitaire (1 bit, 1 octet, …), ou une taille relativement petite.

- RC4: Ron Rivest 1987
- SEAL: Don Coppersmith et Phillip Rogaway pour IBM 1993.

DES

- Blocs 64 bits
- Clé 56 bits
- Conçu par IBM au des années 70 et adopté comme standard officiellement (FIPS46-3) en 1977.
- Permutation initiale + calcul médian en fonction de la clé + permutation finale.

DES

Diviser l'information à crypter en blocs de 8 octets.

Clé DES: chaîne de 64 bits

– 56 bits (clé): 2^{56} clés (~72 millions de milliards possibilités).

– 8 bits restants (8, 16…, 64): bits de parité ou détection d'erreur.

Principe DES:

– clé secrète de 56 bits ===> 16 "sous-clés" de 48 bits chacune.

– 19 Etapes :

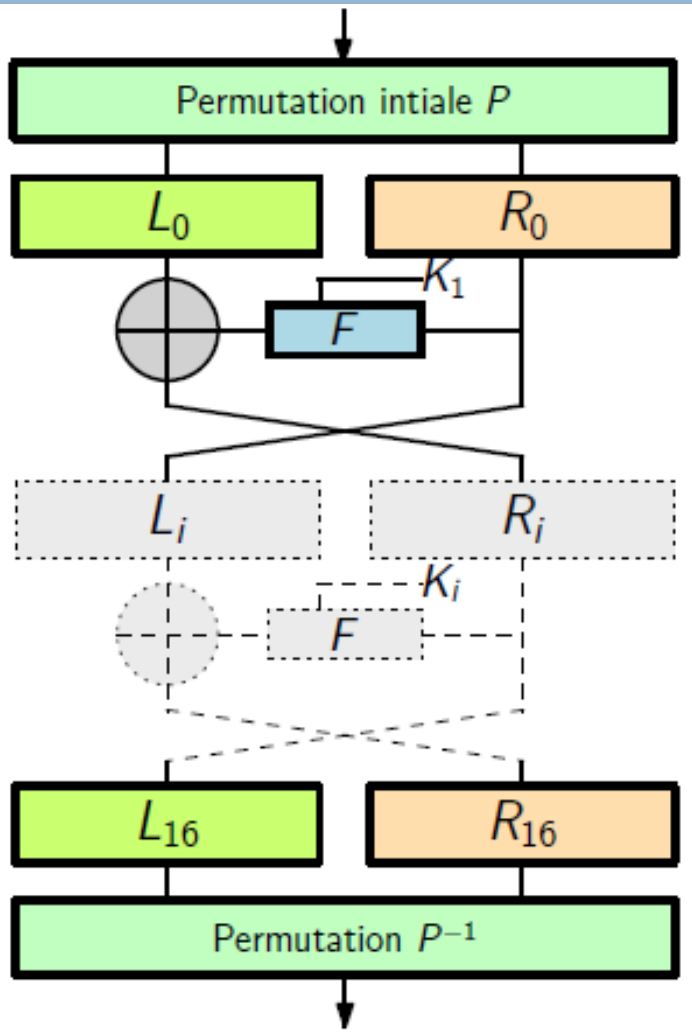
» Etape 1: transposition fixe (standard);

» Etape 2-17 (16): Substitution + Transposition

» Etape 18 et 19: Transposition.

DES

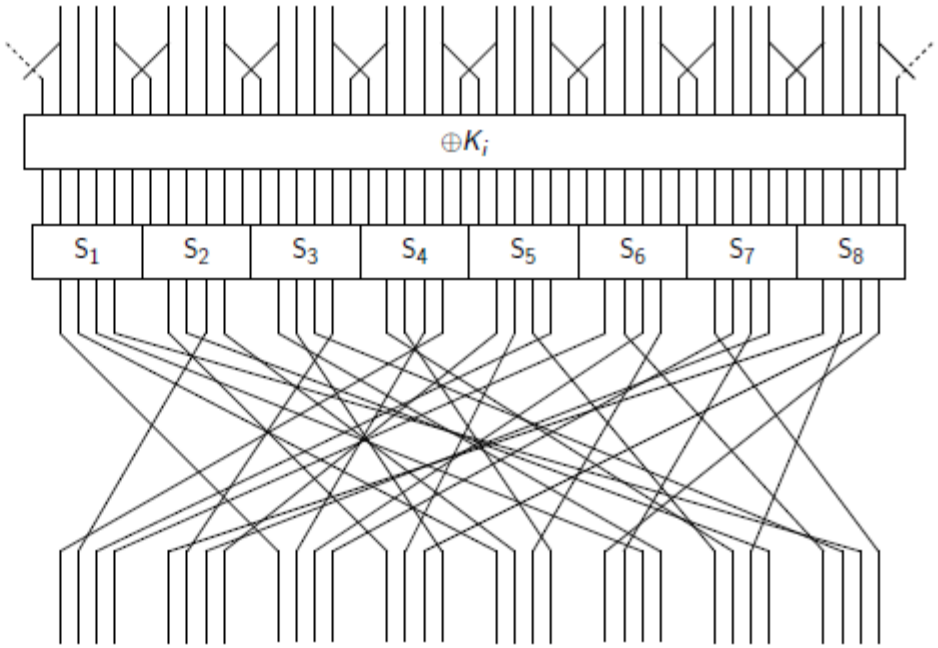
$$L_1 = R_0$$
$$R_1 = L_0 \oplus f(R_0)$$



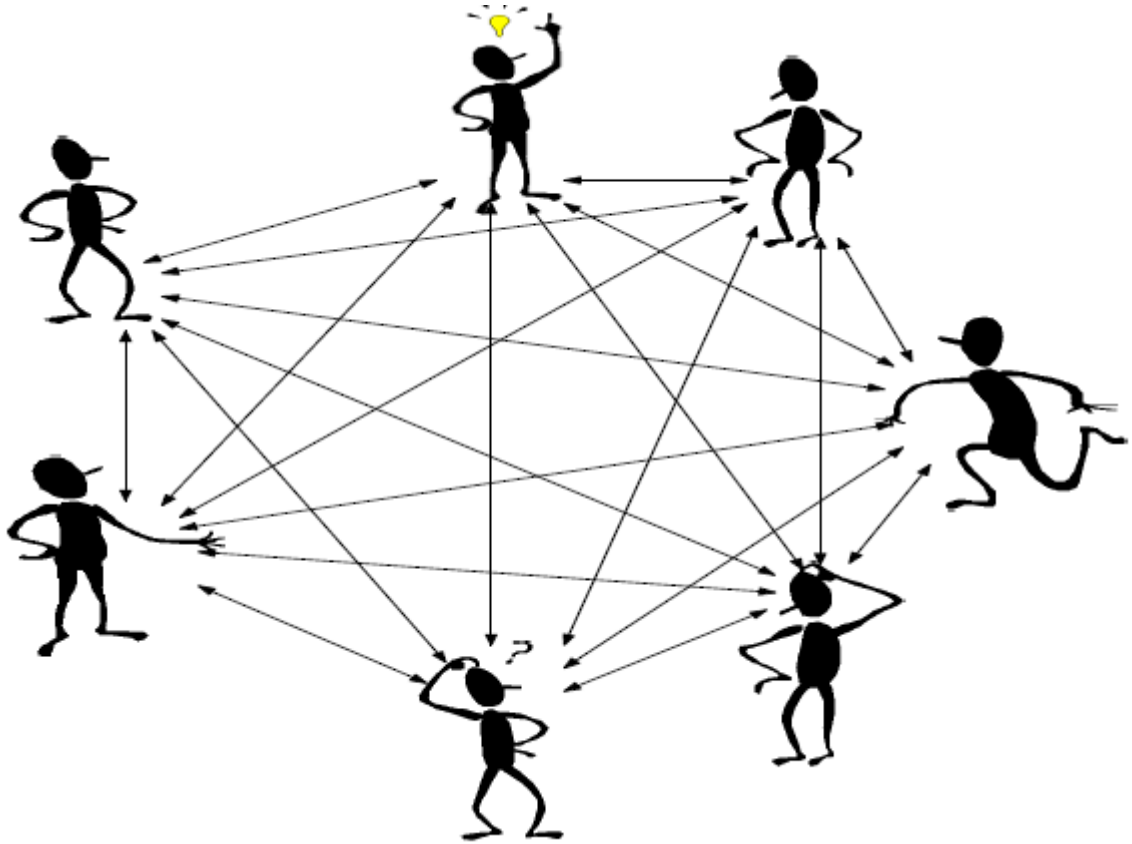
DES

Dans le DES, la fonction f est une fonction de 32 bits vers 32 bits, constituée:

- d'une *expansion* de message de 32 vers 48 bits
- d'un XOR avec 48 bits dérivés de la clé
- de la concatenation de 8 sous-fonctions de 6 vers 4 bits, appelées *boîtes S*
- d'une permutation des 32 bits sortants



Limites de chiffrement symétrique



Algorithmes de chiffrement asymétrique

Implique une paire de clé (SK,PK):

- Une clé publique (PK), publiée dans les annuaires,
- Une clé privé (SK) maintenue secrète chez son propriétaire

Un message chiffré avec la clé publique PK, ne peut être déchiffré qu'avec la clé secrète SK.

RSA: Rivest, Shamir et Adleman 1978

RSA

- Fondé sur la difficulté de factoriser des grands nombres qui sont le produit de deux grands nombres premiers.
- Multiplier deux grands nombres premiers est une fonction à sens unique:
- Il est facile de multiplier deux nombres pour obtenir un produit, mais difficile de factoriser ce produit et de retrouver les deux grands nombres premiers.

RSA

- **Initialisation**

•Choisir deux nombres premiers très grand, p et q.

•Calculer n = p · q (n est le *modulus*).

•Choisir e aléatoire tel que e est premier avec ((p -1) · (q -1))

•Trouver d tel que : ed = 1 mod((p -1)(q -1)).

•Clé publique : (n,e).

Clé privée : (n,d) ou (p,q,d) si on désire garder p et q.

- **Chiffrement/Déchiffrement**

•L'expéditeur crée le texte chiffré c à partir du message m :

$$C = M^e \pmod{n}$$

•Le destinataire reçoit c et effectue le déchiffrement:

$$C^d \bmod n$$

RSA

Alice		Bob
M		
		choisit p et q e premier avec $p-1$ et $q-1$
		calcule $n = p \times q$ d tel que $ed \equiv 1 \pmod{\varphi(n)}$
	$\longleftarrow$	envoie (n, e) à Alice
calcule $C = M^e \pmod{n}$ et l'envoie à Bob	$\longrightarrow$	
		calcule $C^d \pmod{n}$ et en déduit M

Sécurité de RSA

- Clé publique (e,n) connue
- Pour déchiffrer un message m, il faut connaître d
- $ed=1 \mod (p-1)(q-1)$
- Pour calculer d il faut donc connaître p et q
- $n=pq$
- Il faut factoriser n en ses facteurs premiers p et q
- Or personne n'a pus le faire en un temps raisonnable.

Échange de clé Diffie-Hellman

Diffie et Hellman 1976

Objectif:

- Deux entités voudraient se mettre d'accord sur un secret afin de s'échanger des messages confidentiels,

Principe:

- Fondé sur la difficulté du calcul du logarithme discret

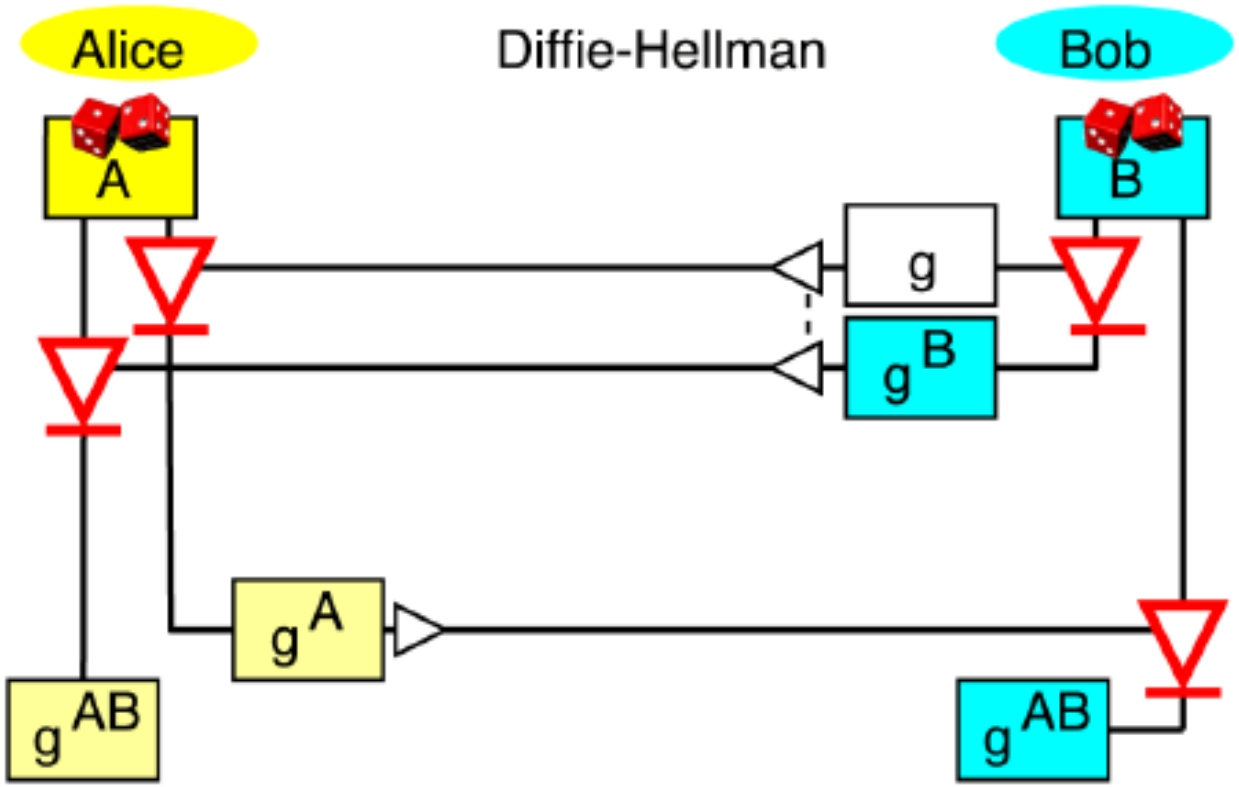
Protocole d'échange de clefs de Diffie-Hellman

- Alice et Bob veulent partager une clef secrète K: On suppose que les données G; $n = |G|$ et g sont publiques.
- Alice choisit un entier $1 \leq a \leq n - 1$ au hasard.
- Alice calcule $A = g^a$ et l'envoie a Bob.
- Bob choisit un entier $1 \leq b \leq n - 1$ au hasard.
- Bob calcule $B = g^b$ et l'envoie a Alice.
- Alice est en mesure de calculer B^a et Bob de calculer A^b . La clef commune est donc
- $K = g^{ab} = A^b = B^a$

Protocole d'échange de clefs de Diffie-Hellman

Alice		Bob
génère a		génère b
$A = g^a \mod p$		$B = g^b \mod p$
	$A \longrightarrow$	
	$\longleftarrow B$	
(dispose de $[a, A, B, p]$)		(dispose de$[b, A, B, p]$
Clé secrète : $K = B^a \mod p$		Clé secrète : $K = A^b \mod p$

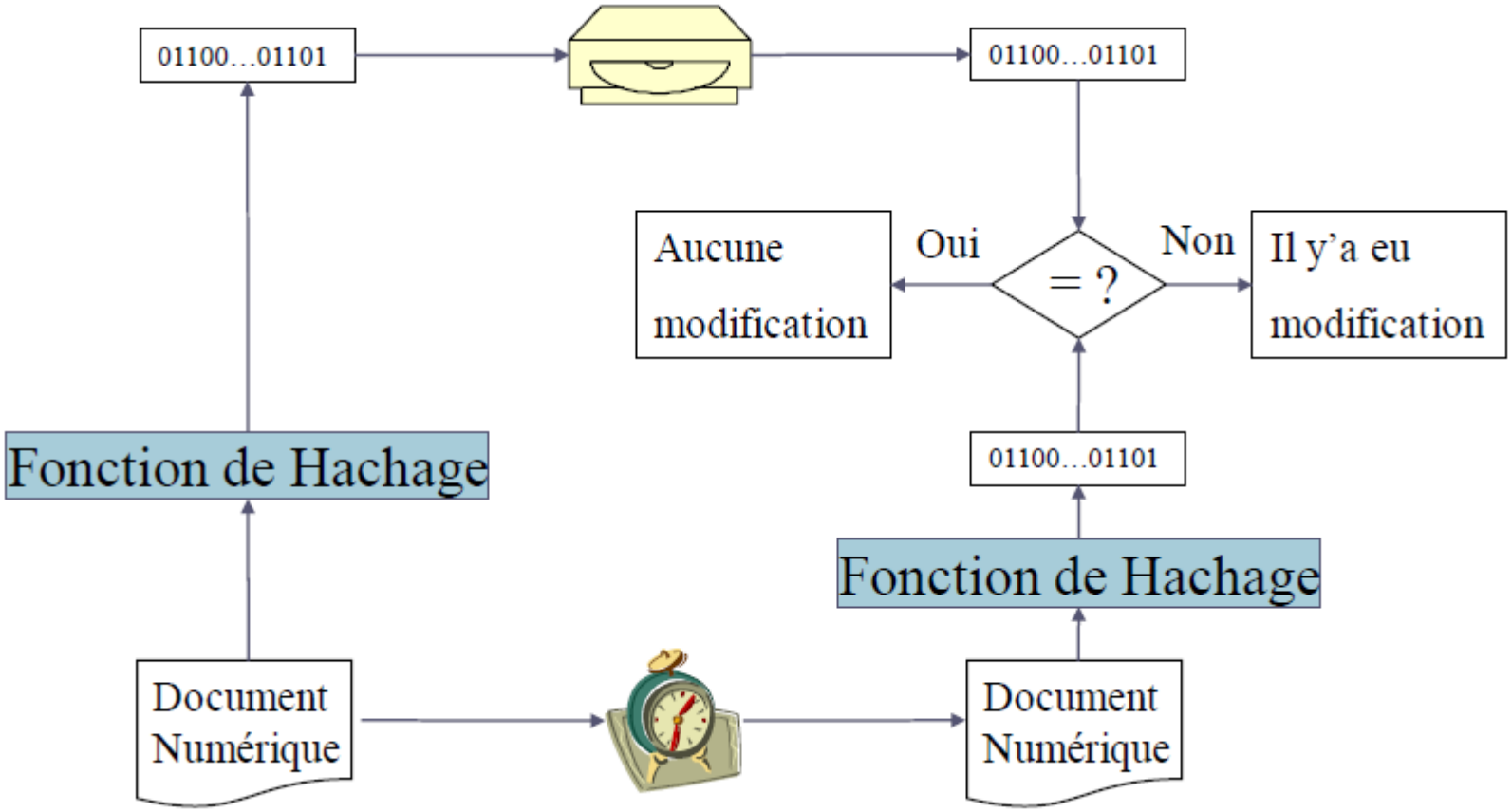
Protocole d'échange de clefs de Diffie-Hellman



Intégrité et fonction de hachage

- L'intégrité : permet de vérifier qu'une données n'a pas été modifiée par une entité tierce (accidentellement ou intentionnellement).
- Une fonction de hachage est typiquement utilisée pour vérifier l'intégrité de données.
- Les fonctions de hachage cryptographique ont les propriétés suivantes:
  - Si on connais m, il est facile de calculer h(m).
  - Si on connais h, il est difficile de calculer m, h=h(m).
  - Si on connais m, il est difficile de trouver un autre message m' tels que h(m) = h(m').

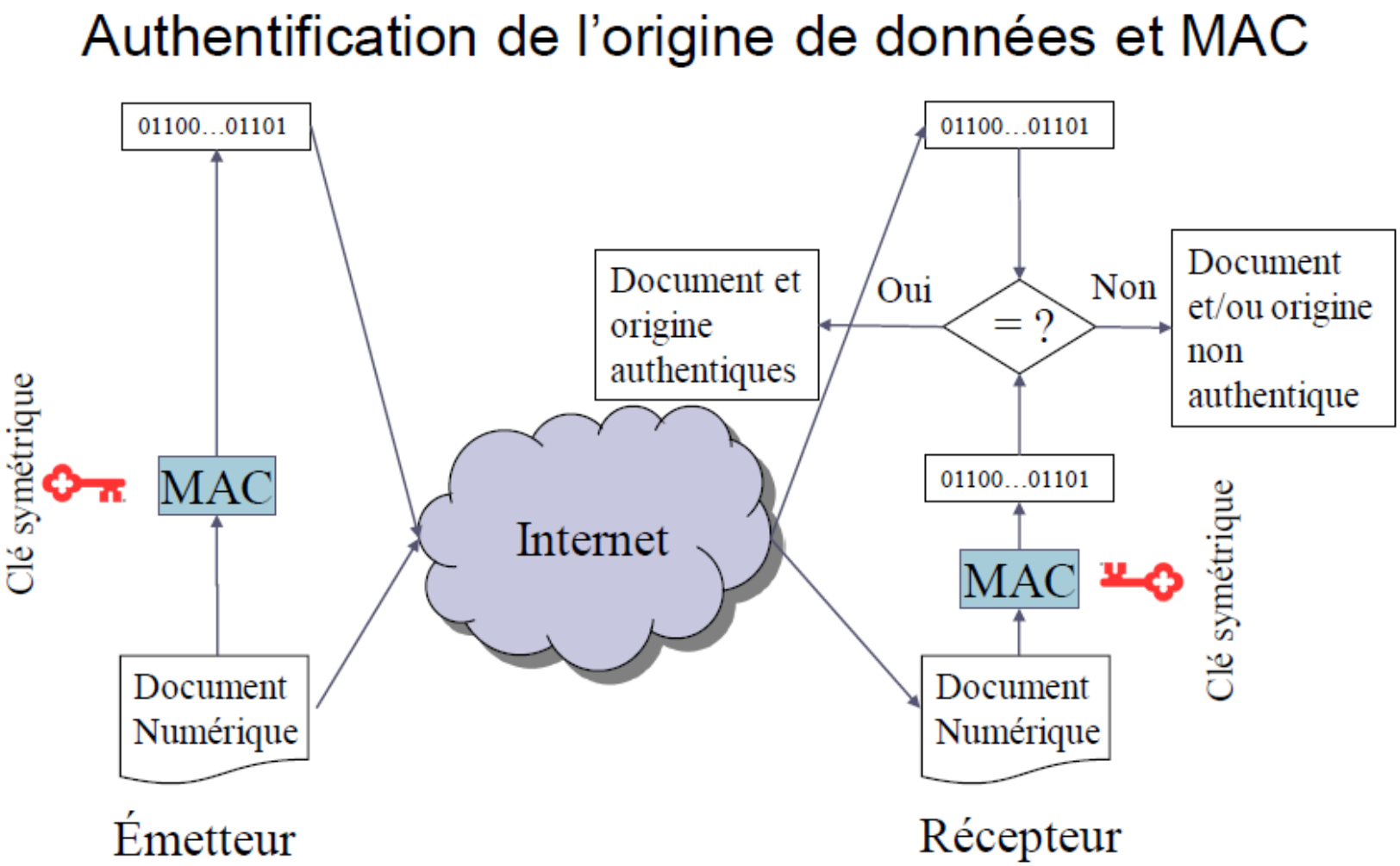
Intégrité et fonction de hachage



Authentification de l'origine de données et MAC

- L'authentification de l'origine de données permet de vérifier que la source de données est bien l'identité prétendue.
- Message Authentication Code (MAC) est un mécanisme cryptographique qui permet de vérifier l'authenticité de l'origine des données et leur intégrité en même temps.
- Un algorithme MAC est une fonction de hachage paramétré par une clé k possède les propriétés suivantes:
  - Si m et k sont connus, il est facile de calculer H_k (m).
  - Si plusieurs pairs (m_i, $H_k(m_i)$) sont connus, il est difficile de calculer le pair (m, H_k(m)) pour un nouveau m.

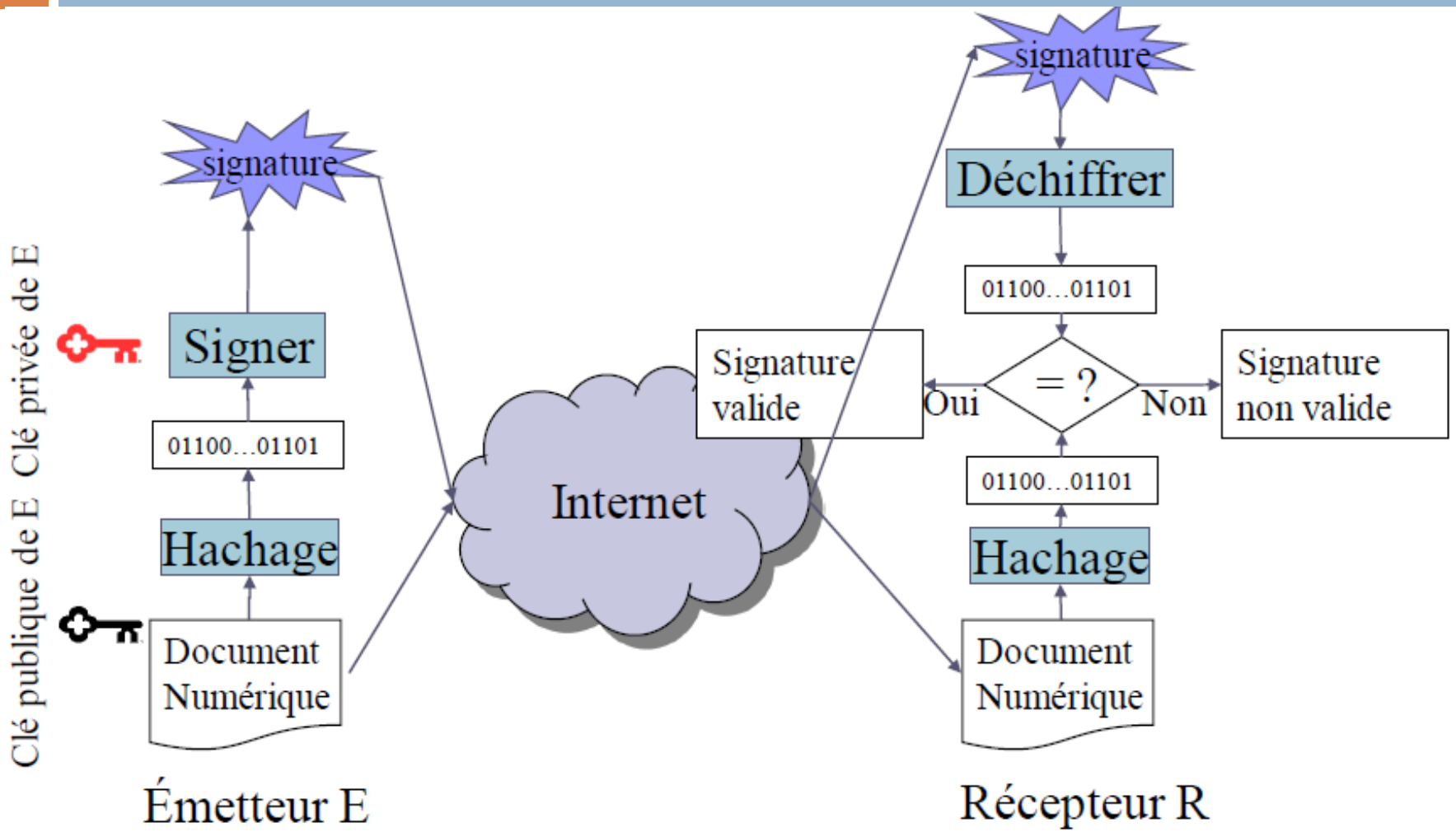
Authentification de l'origine de données et MAC



Non répudiation de l'origine

- La non répudiation de l'origine assure que l'émetteur du message ne pourra pas nier avoir émis le message dans le futur.
- La signature digitale est un mécanisme cryptographique qui permet d'assurer la non répudiation de l'origine.
- Repose sur un système cryptographique asymétrique
- La signature est calculée en utilisant la clé privé
- La signature est vérifiée en utilisant la clé publique

Signature digitale et non répudiation de l'origine



Signature digitale avec RSA

- **Initialisation**

•Choisir deux nombres premiers, p et q, les deux étant plus grands que 10^{100}

•Calculer n = p · q (n est le *modulus)*

•Choisir e aléatoire tel que e et ((p -1) · (q -1)) n'aient aucun facteur commun excepté 1

•Trouver d tel que : ed = 1 mod((p -1)(q -1)).

•Clé publique : (n,e).

Clé privée : (n,d) ou (p,q,d) si on désire garder p et q.

- **Signature digitale**

•L'expéditeur crée la signature s à partir du message m :

$s = m^d \bmod(n)$, où (n,d) est la clé privée de l'expéditeur.

•Le destinataire reçoit s et m et effectue la vérification de m:

$m = s^e \bmod(n)$, où (n,e) est la clé publique de l'expéditeur.