Deuxième partie

Cryptographie

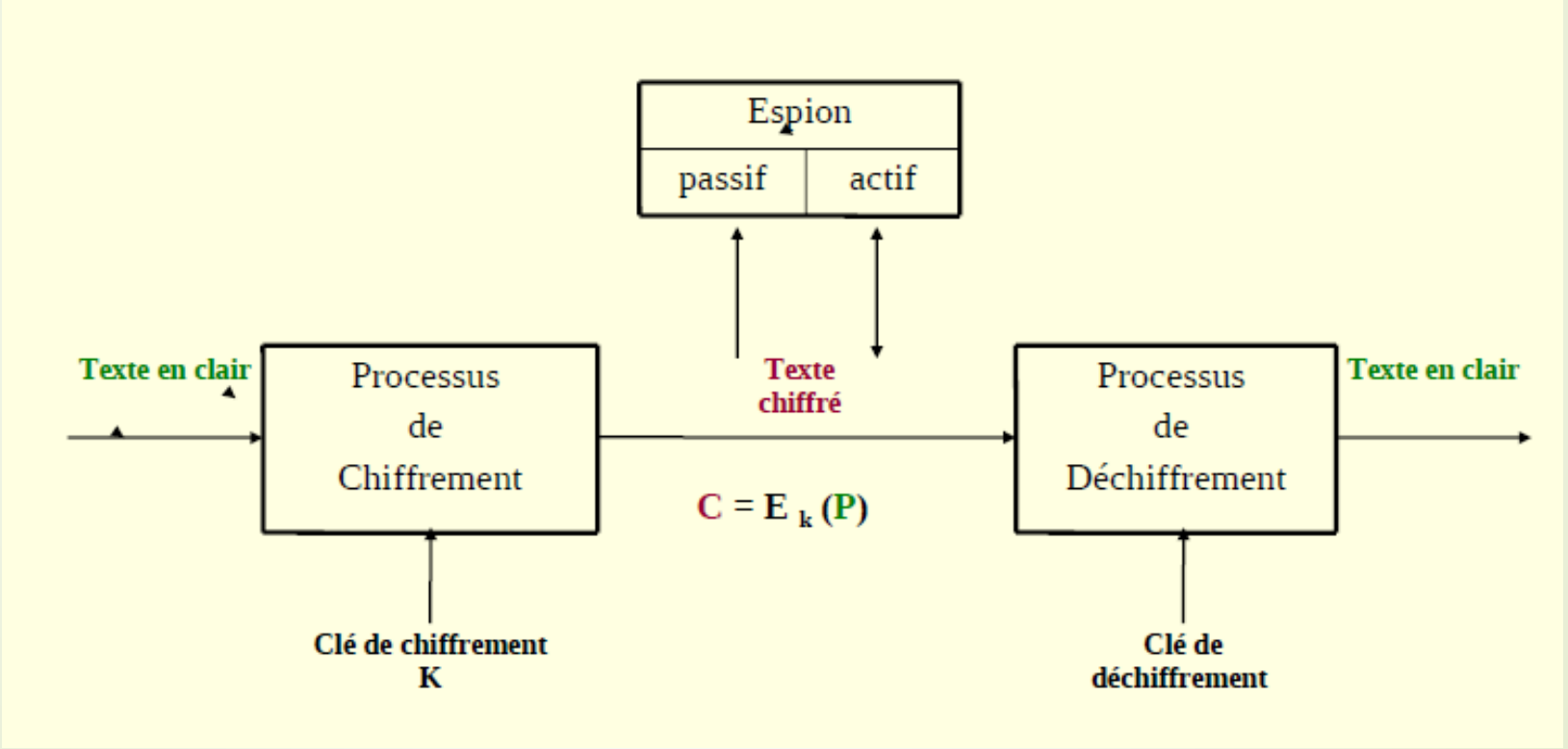
Introduction

- La cryptographie est l'art de transformer un message clair en un message inintelligible par celui qui ne possède pas les clefs de chiffrement.
- La cryptographie nous permet de stocker des informations sensibles ou de les transmettre à travers des réseaux non sûrs (comme Internet) de telle sorte qu'elles ne puissent être lues par personne à l'exception du destinataire convenu.
- La cryptographie de garantir :
- Confidentialité : lisible uniquement par les personnes autorisées,
- authenticité : être sûr de son origine,
- intégrité : être sûr qu'il n'a pas été modifié (intentionnellement ou accidentellement).
- Non répudiation:

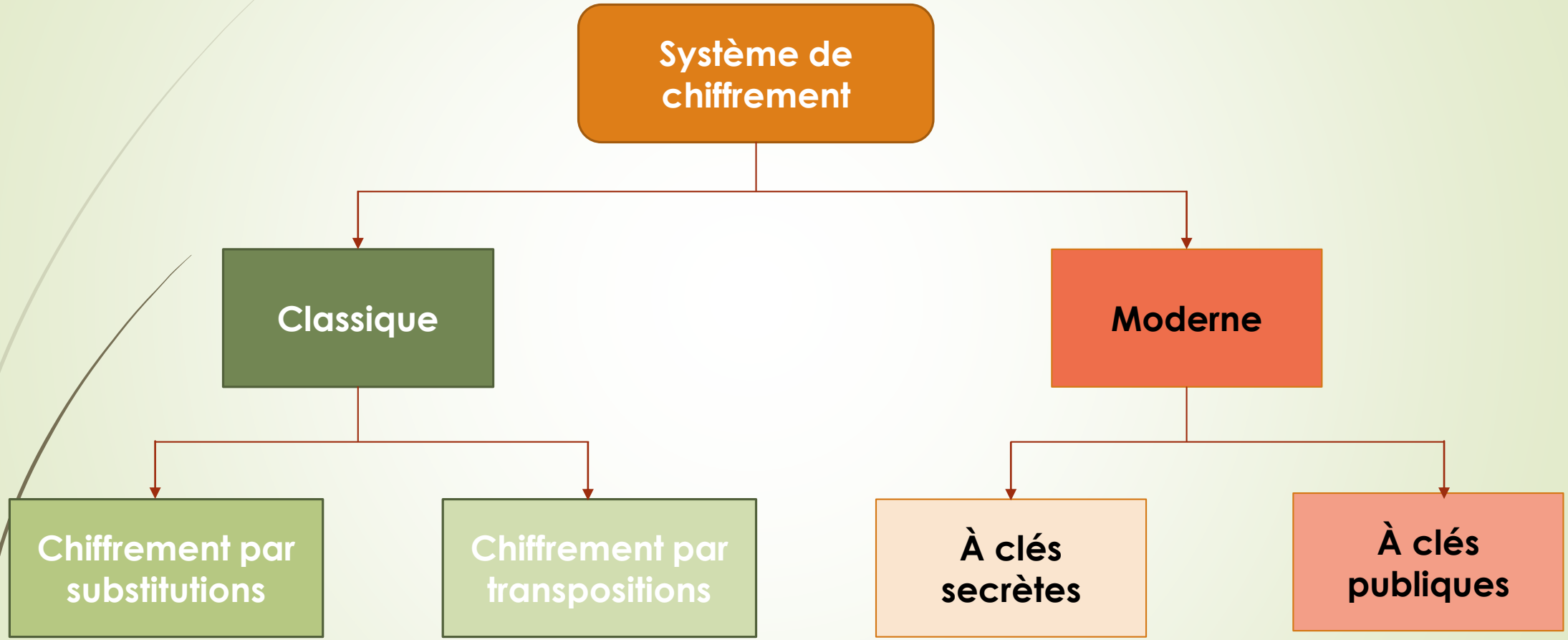
Vocabulaire

- **Chiffrement :** opération qui consiste à rendre le document illisible pour toute personne non autorisée.
- **Clé :** paramètre utilisé en entrée d'une opération cryptographique.
- **Déchiffrement :** opération qui consiste à rendre le document chiffré en document original (lisible).
- **Cryptanalyse :** opération qui consiste à rendre le document chiffré en document lisible sans avoir la clé.
- **Message clair :** Message lisible.
- **Message chiffré :** Message illisible, également appelé cryptogramme.

Principe du chiffrement



Méthodes de chiffrement



Chiffrement classique :

Chiffrement par substitution

- **Substitution mono alphabétique**

- Le chiffrement monoalphabétique ou chiffrement par substitution est une des plus anciennes méthodes de chiffrement. Elle consiste à remplacer chaque lettre d'un texte par un symbole donné (ce symbole peut être une autre lettre de l'alphabet). Sachant que deux lettres distinctes doivent être chiffrées en deux signes distincts pour permettre un déchiffrement du message sans ambiguïté.

Chiffrement classique :

Chiffrement par substitution

- **Substitution mono alphabétique**
- **Code secret de Jules César:**
  - Chiffrement par substitution une lettre en remplace une autre
  - Exemple très simple de cryptographie conventionnelle :

✓ Algorithme : décalage des lettres de l'alphabet

✓ Clé : nombre de lettre de décalage

– Si on utilise 3 comme valeur de la clé la lettre A est remplace par *D*, B par *E*, C par *F* etc. :

ABCDEFGHIJKLMNOPQRSTUVWXYZ

DEFGHIJKLMNOPQRSTUVWXYZABC

Chiffrement classique :

Chiffrement par substitution

- **Substitution mono alphabétique**
- **Code secret de Jules César**

Exemple de codage :

- Texte clair : cryptographie cesar
- Clé=2
- Texte chiffre : etarvqitcrjkg eguct

Chiffrement classique :

Chiffrement par substitution

- **Substitution polyalphabétique**

- La substitution **polyalphabétique** consiste à 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. ... Pour **chiffrer** la lettre suivante on utilise alors le caractère suivant de la clé et ainsi de suite.

Chiffrement classique :

Chiffrement par substitution

- **Substitution polyalphabétique**
  - Code de ***Vigenère*** (vers 1560)

✓ Amélioration du code de César

✓ Utilisation de 26 alphabets décalés (versus 1 dans le code de César)

✓ Clé : définit le décalage pour chaque lettre du message

✓ Avantage : différentes occurrences de la même lettre du message pourront être codée de façon différente

✓ Exemple

Texte clair	C	H	I	F	F	R	E	D	E	V	I	G	E	N	E	R	E
Clé	I	U	P	M	I	A	G	E	I	U	P	M	I	A	G	E	I
Décalage	8	20	15	12	8	0	6	4	8	20	15	12	8	0	6	4	8
Texte crypté	*K*	*B*	*X*	*R*	*N*	*R*	*K*	*H*	*M*	*P*	*X*	*S*	*M*	*N*	*K*	*V*	*M*

Chiffrement classique :

Chiffrement par substitution

- **Substitution polyalphabétique**
  - **Code de Hill:** publié en 1929 par **Lester S. Hill**
  - **Principe de chiffrement :**
  - Les lettres sont d'abord remplacées par leur rang dans l'alphabet. Les lettres P_k et P_{k+1} du texte clair seront chiffrées C_k et C_{k+1} avec la formule ci-dessous:

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

Ce qui signifie, pour fixer les idées, que les deux premières lettres du message clair (P_1 et P_2) seront chiffrées (C_1 et C_2) selon les deux équations suivantes:

$$C_1 \equiv aP_1 + bP_2 \pmod{26}$$

$$C_2 \equiv cP_1 + dP_2 \pmod{26}$$

Chiffrement classique :

Chiffrement par substitution

- **Substitution polyalphabétique**
  - **Code de Hill:**

Exemple de chiffrement

- **K=** $\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$, **M=** je vous aime
- Après avoir remplacé les lettres par leur rang dans l'alphabet (a=1, b=2, etc.), elle obtiendra:

$$C_1 \equiv 9 \cdot 10 + 4 \cdot 5 \pmod{26} = 110 \pmod{26} = 6$$
$$C_2 \equiv 5 \cdot 10 + 7 \cdot 5 \pmod{26} = 85 \pmod{26} = 7$$

Elle fera de même avec les 3e et 4e lettres, 5e et 6e, etc. Elle obtiendra finalement:

Lettres	j	e	v	o	u	s	a	i	m	e
Rangs (Pk)	10	5	22	15	21	19	1	9	13	5
Rangs chiffré (Ck)	6	7	24	7	5	4	19	16	7	22
Lettres chiffrée	f	g	x	g	e	d	s	p	g	v

Chiffrement classique :

Chiffrement par substitution

- **Masque jetable :** également appelé **chiffre de Vernam**, est le seul algorithme de cryptage connu comme étant indécryptable. C'est en fait un chiffre de Vigenère avec comme caractéristique que la clef de chiffrement a la même longueur que le message clair. Le système du masque jetable fut inventé par **Gilbert Vernam** en 1917

Le chiffrement par la méthode du masque jetable consiste à combiner le message en clair avec une clé présentant les caractéristiques très particulières suivantes :

- La clé doit être une suite de caractères au moins aussi longue que le message à chiffrer.
- Les caractères composant la clé doivent être choisis de façon totalement aléatoire.
- Chaque clé, ou « masque », ne doit être utilisée qu'une seule fois (d'où le nom de *masque jetable*).

Chiffrement classique :

Codes de transposition

- Algorithme : change l'ordre des lettres (mais ne les masque pas)
- Transposition par colonnes

M	I	A	G	E
5	4	1	3	2
e	x	e	m	p
l	e	d	e	c
o	d	e	u	t
i	l	i	s	a
n	t	l	a	t
r	a	n	s	p
o	s	i	t	i
o	n	p	a	r
c	o	l	o	n
n	e	s	a	b

Clé : MIAGE
Colonnes numérotées dans l'ordre alphabétique des lettres de la clé

Texte en clair :
exempledecodeutilisantlatransp
ositionparcolonnes

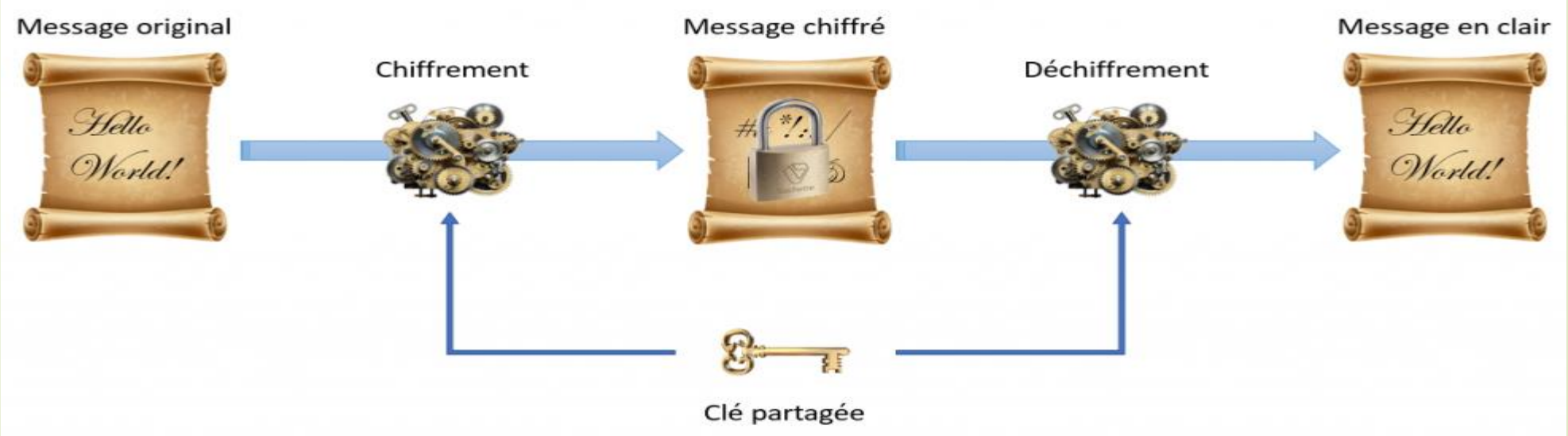
Texte encrypté :

edeilniplspctatpirnbmeusastaoa
xedltasnoeeloinroocn

Chiffrement moderne

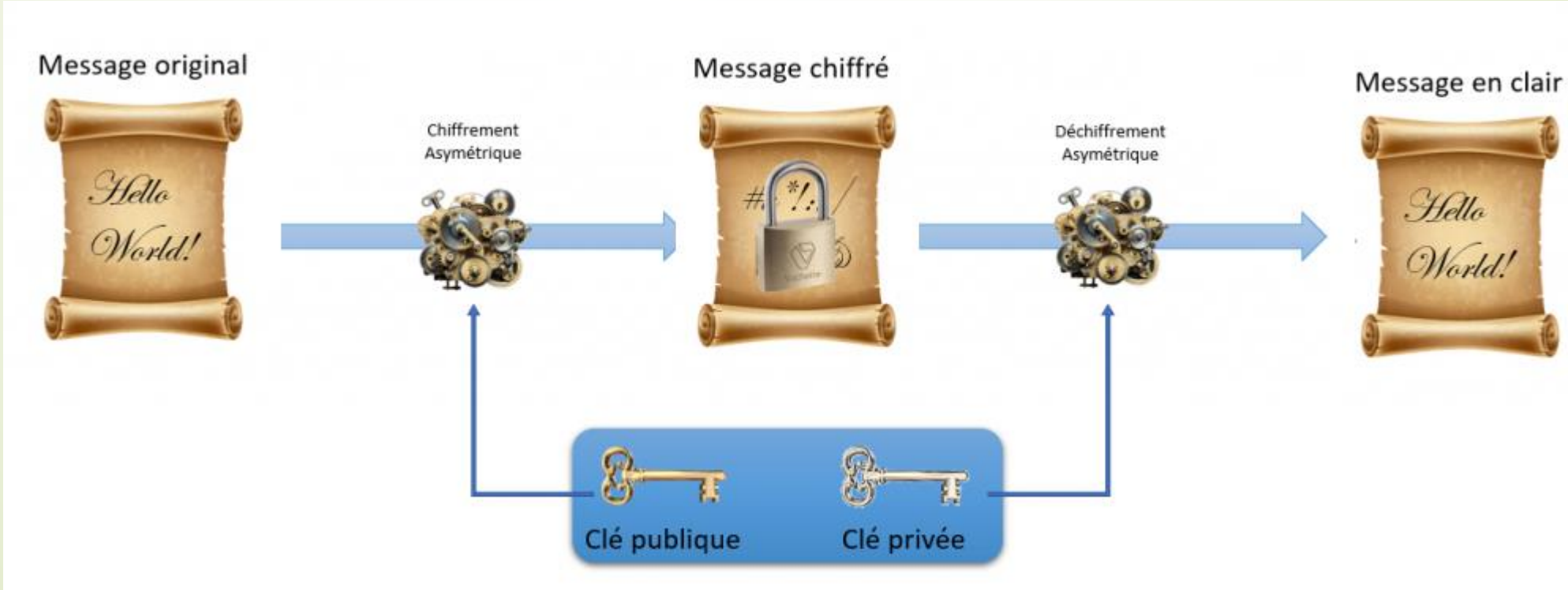
Classes de chiffrement moderne

- **Chiffrement symétrique:** appelé également chiffrement à clé secrète. Une seule clé partagée qui sert au chiffrement et au déchiffrement



Classes de chiffrement moderne

- **Chiffrement asymétrique:** appelé également chiffrement à clé publique. Une clé publique est utilisée au chiffrement et une autre clé dite privée est utilisée au déchiffrement



Chiffrement symétrique

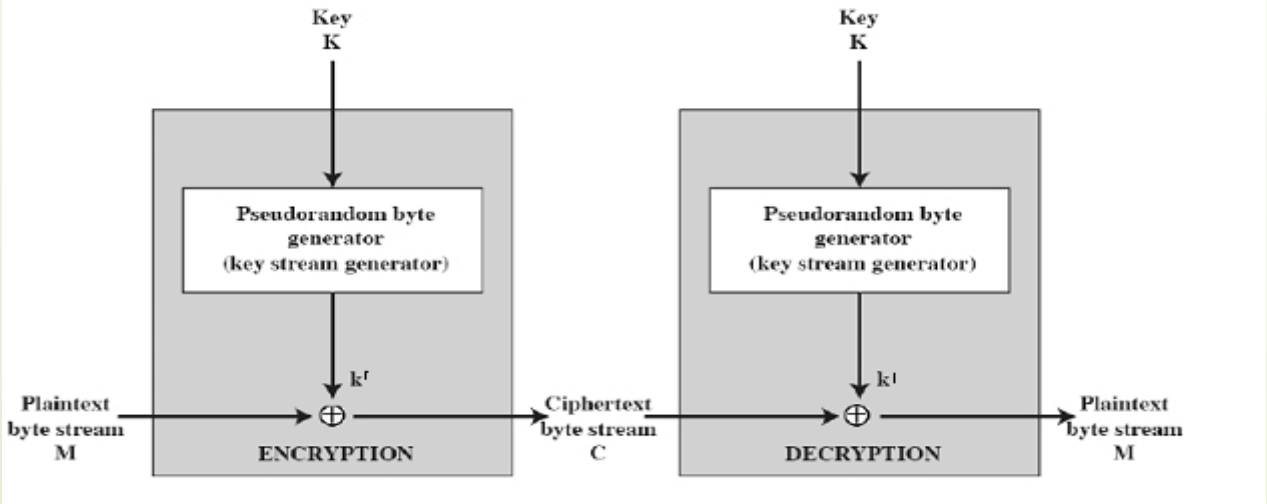
Classes de chiffrements symétriques:

- Chiffrement symétrique par flot
- Chiffrement symétrique par bloque

Chiffrement symétrique
Système de chiffrement par flot

Chiffrement symétrique par flot

- Traitement à la volée ; chiffrement à la one-time pad : $|M| = n$ et avec une petite clé K, générer $K'/|K'| = n$
- Sécurité :
  - Substitution rapide ($\oplus$ typiquement)
  - Générateur pseudo aléatoire : impossible à prédire
- Ex : LFSR, RC4 (Rivest), E0[Bluetooth],A5/1[GSM]



Chiffrement symétrique
Système de chiffrement par blocs

Définition

- On désigne par chiffrement par blocs (block-cipher en anglais), tout système de chiffrement (symétrique) dans lequel le message clair est découpé en blocs d'une taille fixe, et chacun de ces blocs est chiffre.
- La longueur n des blocs et la taille l des clés sont deux caractéristiques des systèmes de chiffrement par blocs.

Chiffrement symétrique
Système de chiffrement par blocs

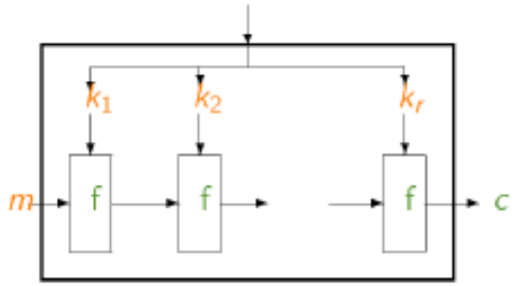
Découpage en blocs

- Le message m a chiffrer est découpé en blocs de n bits.
- m = m1m2…mk :
- Si la longueur du message n'est pas un multiple de la longueur d'un bloc, on le complète : c'est le bourrage ou padding en anglais.
- Plusieurs techniques de bourrage existent.

Chiffrement symétrique
Système de chiffrement par blocs

Chiffrement itératif

- Tous les sytèmes de chiffrement par blocs actuels suivent le schéma suivant



- Le bloc clair m est transformé r fois successivement à l'aide d'une fonction f qui dépend d'une sous-clé k_i . Le chiffré c est le résultat de la dernière transformation.

$$c = f(...f(f(m, k_1), k_2), ...), k_r).$$

r est appelé nombre de tours ou de rondes.

Chiffrement symétrique
Système de chiffrement par blocs

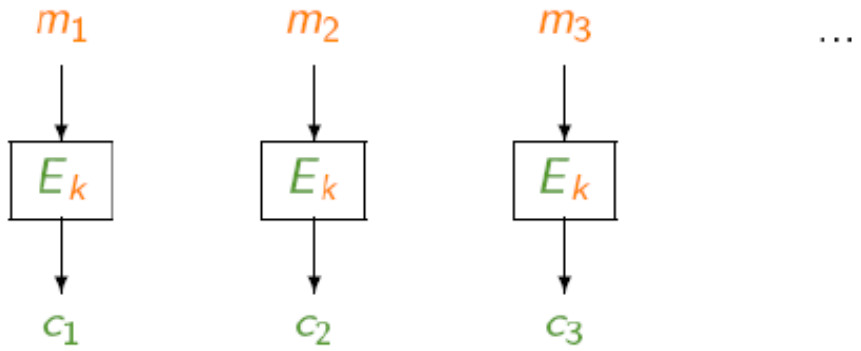
- Sécurité : dépend du mode de chiffrement !
- Ex : DES, AES, IDEA, BLOWFISH, RC6

Chiffrement symétrique
Système de chiffrement par blocs

Les modes de chiffrement

Le mode ECB

- Mode ECB (Electronic Code Book)
  - Chiffrement : chaque bloc clair m_i est chiffré indépendamment et donne un bloc chiffré $c_i = E_k(m_i)$.
  - Déchiffrement : chaque chiffré est déchiffré indépendamment pour donner le clair correspondant $m_i = D_k(c_i)$.
  - Conséquence : deux blocs clairs identiques donnent toujours le même bloc chiffré pour une clé k fixée.
  - Aucune sécurité, pas d'utilisation

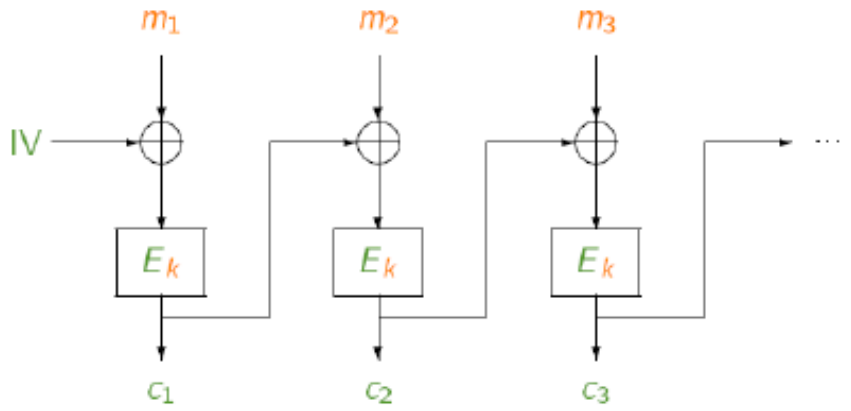


Chiffrement symétrique
Système de chiffrement par blocs

Les modes de chiffrement

Le mode CBC

- Mode CBC (Cipher Bloc Chaining)
  - Chiffrement : un vecteur d'initialisation IV est généré aléatoirement. $c_i = E_k(m_i \oplus c_{i-1})$. Le vecteur IV est transmis avec les blocs chiffrés.
  - Déchiffrement : $m_i = D_k(c_i) \oplus c_{i-1}$.
  - Conséquence : deux blocs clairs identiques chiffrés différemment.
  - Mode le plus utilisé

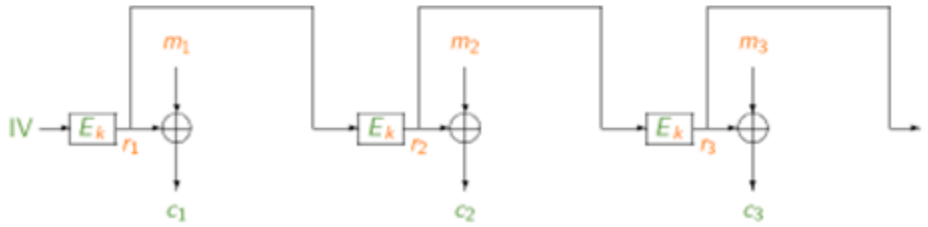


Chiffrement symétrique
Système de chiffrement par blocs

Les modes de chiffrement

Le mode OFB

- Mode OFB (Output FeedBack)
  - Chiffrement : un vecteur d'initialisation IV est généré aléatoirement. $c_i = r_i \oplus m_i$, où $r_0 = IV$ et pour $i \geq 1$, $r_i = E_k(r_{i-1})$. Le vecteur IV est transmis avec les blocs chiffrés.
  - Déchiffrement : $m_i = c_i \oplus r_i$.
  - Conséquence : deux blocs clairs identiques chiffrés différemment.

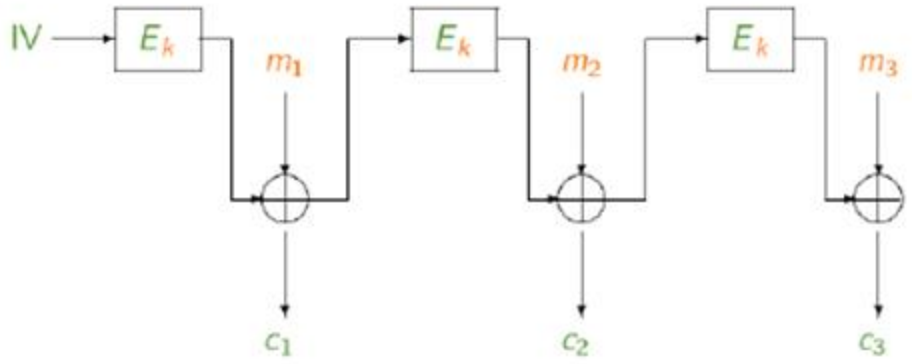


Chiffrement symétrique
Système de chiffrement par blocs

Les modes de chiffrement

Le mode CFB

- Mode CFB (Cipher FeedBack)
  - Chiffrement : un vecteur d'initialisation IV est généré aléatoirement. $c_i = r_i \oplus m_i$, où $r_1 = E_k(IV)$ et pour $i \geq 2$, $r_i = E_k(m_{i-1} \oplus r_{i-1})$. Le vecteur IV est transmis avec les blocs chiffrés.
  - Déchiffrement : $m_i = c_i \oplus r_i$.
  - Conséquence : deux blocs clairs identiques chiffrés différemment.

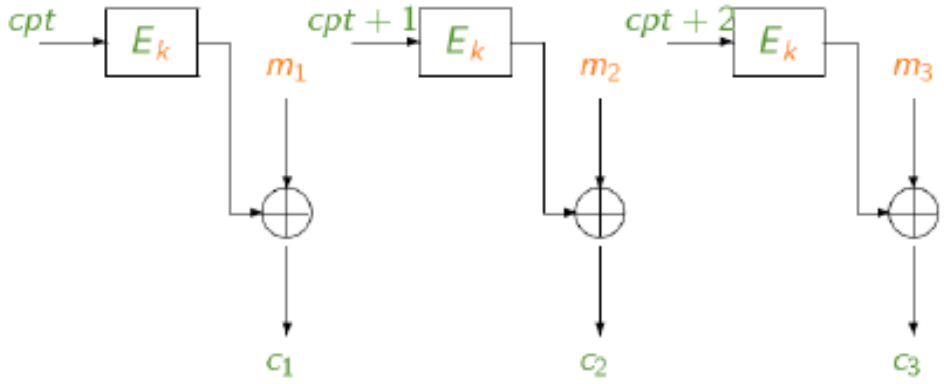


Chiffrement symétrique
Système de chiffrement par blocs

Les modes de chiffrement

Le mode CTR

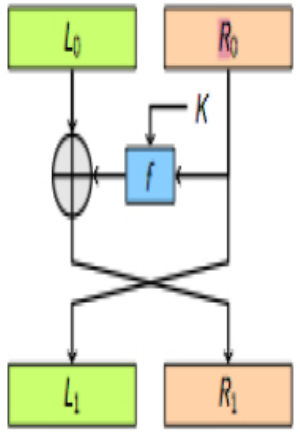
- Mode CTR (CounTeR mode)
  - Chiffrement : $c_i = r_i \oplus m_i$, où $r_1 = E_k(cpt)$ et pour $i \geq 2$, $r_i = E_k(cpt + i - 1)$.
  - Déchiffrement : $m_i = c_i \oplus r_i$.
  - Conséquence : deux blocs clairs identiques chiffrés différemment.



Chiffrement symétrique
Système de chiffrement par blocs

Réseau de Feistel

- Base de pratiquement tous les algorithmes modernes à clé secrète (en particulier DES)
  Proposé par Horst Feistel (IBM) en 1973
- Système de chiffrement par blocs
- Chiffrement et déchiffrement structurellement identiques



Nous avons :

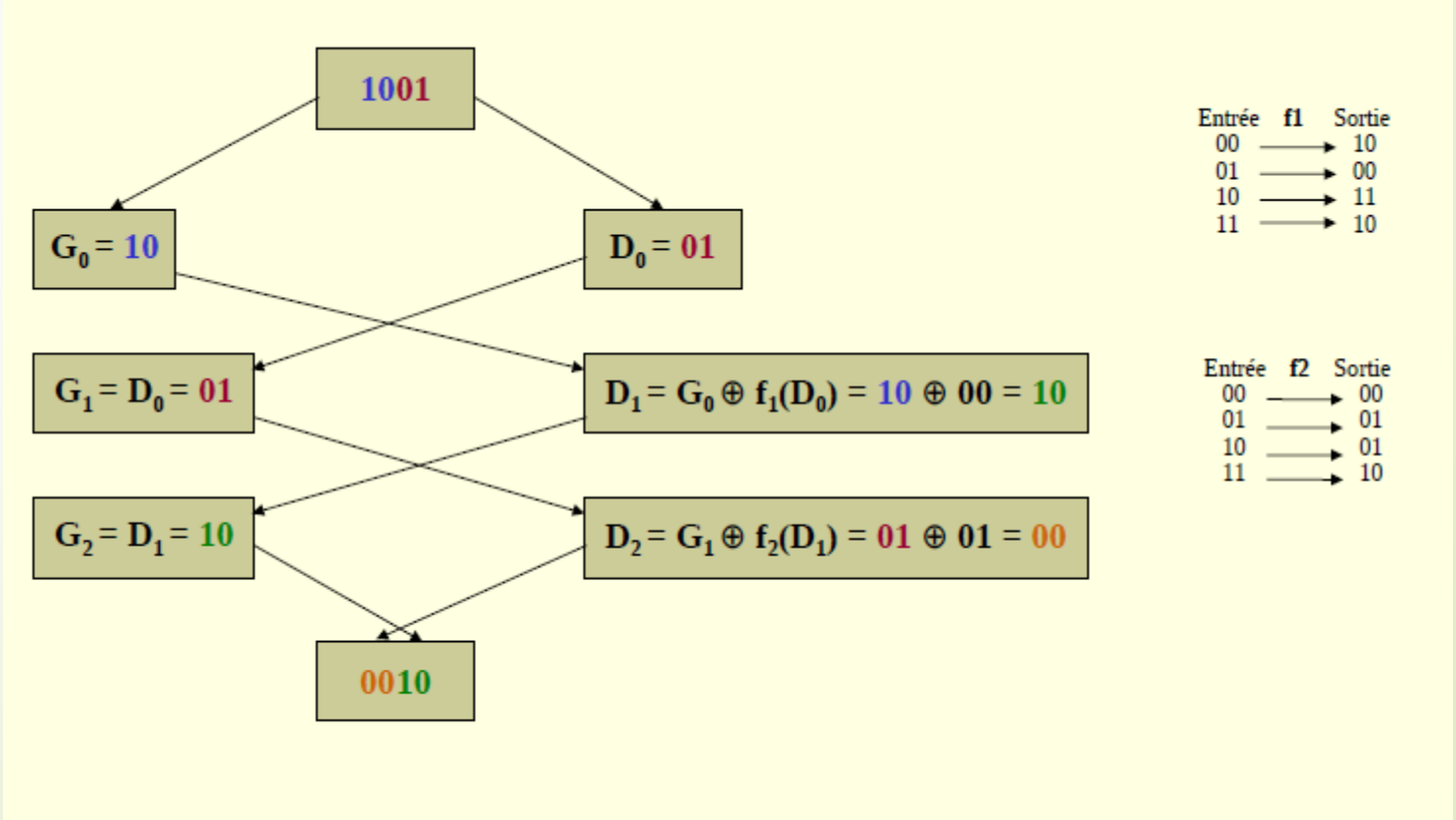
$$\begin{cases} L_1 = R_0 \\ R_1 = L_0 + f(R_0, K) \end{cases}$$

Ainsi :

$$\begin{cases} R_0 = L_1 \\ L_0 = R_1 - f(L_1, K) \end{cases}$$

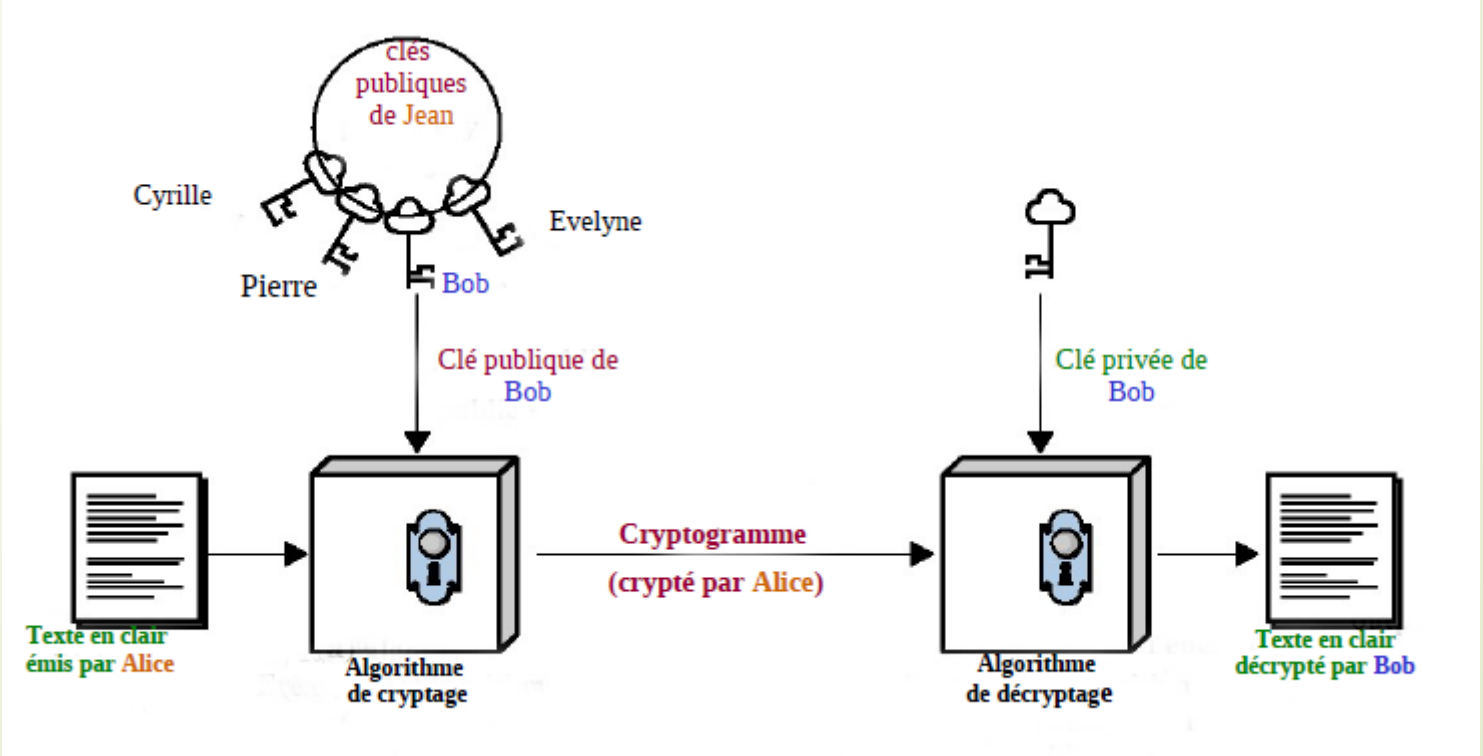
Chiffrement symétrique
Système de chiffrement par blocs

- **Réseau de Feistel: exemple simplifié**



Chiffrement à clé publique

- **Modèle de cryptage à clé publique**



Chiffrement à clé publique

Algorithme RSA

- RSA : méthode proposée pour choisir les clés par Rivest, Shamir et Adelman du MIT (Massachusetts Institute of Technology) en 1978
- La sécurité repose sur la difficulté de factoriser un nombre qui est le produit de deux nombre premiers très grands.
- Les clés publique et privée sont générées à partir de deux nombres premiers très grands (plus de 100 chiffres)

Chiffrement à clé publique

Algorithme RSA

- Principe
  - Prendre 2 nombres premiers très grands : p et q
  - Calculer $n = p \times q$
  - Calculer $z = \Phi(n) = (p-1) \times (q-1)$
  - Prendre un nombre e premier avec z :
    PGCD $(z,e) = 1$ avec $1 < e < z$
  - Calculer d tel que $d \times e = 1 \bmod z$
  - La clé publique correspond au couple : $\{e,n\}$
  - La clé privé correspond au couple : $\{d,n\}$

Chiffrement; $C=M^e \bmod (N)$

Déchiffrement: $M=C^d \bmod (N)$

Chiffrement à clé publique

Algorithme RSA

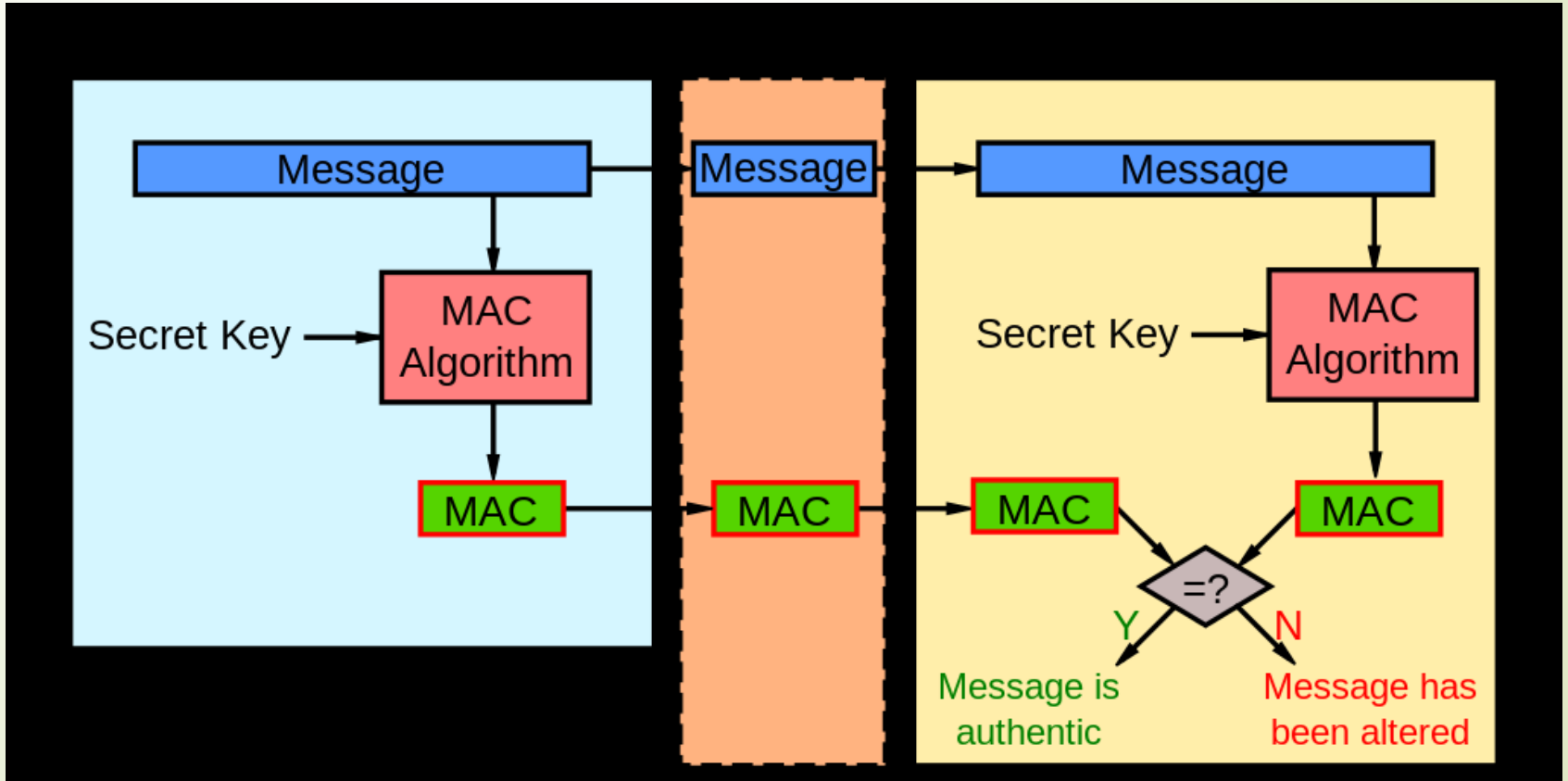
- Exemple simplifié (avec p et q très petits)
  - On choisit : $p = 5$ et $q = 11$
  - Ce qui implique :
    - ✓ $\boldsymbol{n} = p \times q = 5 \times 11 = 55$
    - ✓ $z = \Phi(n) = (p-1) \times (q-1) = 4 \times 10 = 40$
  - On peut choisir $e = 7$ (7 est premier avec 40)
    - ✓ Et on calcule d tel que :
      $d \times e = 1 \bmod z \Rightarrow d \times 7 = 1 \bmod 40 \Rightarrow d = 23$
  - On obtient donc :
    - ✓ Clé publique : {7, 55}
    - ✓ Clé privée : {23, 55}

La Cryptographie au Service de La Sécurité Informatique

- **Les codes d'authentification de message – MAC**
- Les codes d'authentification de message, plus connus sous l'acronyme MAC, de l'anglais **M**essage **A**uthentification **C**ode, sont des fonctions cryptographiques destinées à vérifier l'intégrité de données
- ils calculent à partir d'un message de longueur arbitraire un résumé de longueur fixe (on appelle ce résumé un haché)

La Cryptographie au Service de La Sécurité Informatique

- Contrôle d'intégrité



La Cryptographie au Service de La Sécurité Informatique

Signature électronique

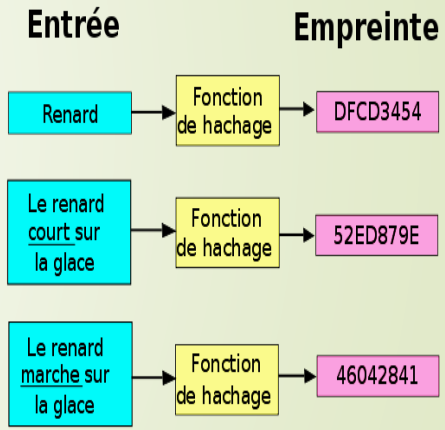
- Une signature numérique est un mécanisme de cryptographie utilisé pour vérifier l'authenticité et l'intégrité de données numériques.

- **Elle se base sur la cryptographie à clé publique et utilise les fonctions de hachage**

La Cryptographie au Service de La Sécurité Informatique

Fonction de hachage

- **Fonction de hachage**: Une fonction **H** qui prend en entrée un message d'une taille arbitraire, et retourne un message appelé *empreinte* ou *haché h* de taille fixe *l*= 160, 256, 384, 512, ... bits



- **H**: {0, 1}* --> {0, 1}^{l}

- Propriétés
  - *Calculabilité*: étant donnée M, il est facile de calculer *h*=H(M)
  - *Irréversible*: étant donnée un haché *h*, il est *impossible en pratique* de trouver M tel que H(M)=*h*
  - *Résistance aux collisions:* Il est *impossible en pratique* de trouver deux messages M, M' tel que H(M)=H(M')

- Exemples: *MD4, MD5 (128 b), SHA-1 (160 b), SHA-256/384/512,* fonctions de hachage publique

- Est ce que la longueur du haché à une quelconque influence?

La Cryptographie au Service de La Sécurité Informatique

- Intégrité, Authentification et non répudiation