Module: Cryptographie

3ème année licence en Informatique

Par : Prof. Cherif Foudil

Module: **Cryptographie**

Plan

Contenu de la matière :

1- Initiation aux concepts fondamentaux et aux méthodes de la cryptographie contemporaine(classique).

2- Principes de la cryptographie à clef publique, ses avantages par rapport à la cryptographie classique qui oblige à garder secrètes les clefs de chiffrement et de déchiffrement.

3- Etude de quelques cryptosystèmes tels que le célèbre RSA, et protocoles d'échanges de clefs, d'authentification, de chiffrement.

4- Gestion des clés et fonction de hashage.

Suite

Plan

- 1 Cours + 1 TD

- Evaluation :

Examen:	50%
TD: (3 interrogations)	50%

- **Présence au cours est obligatoire**

Plan du cours

Plan

Chapitre 1 : Introduction

Chapitre 2: Concepts mathématiques

Chapitre 3: Principe de la cryptographie

Partie 1: Cryptographie classique

Partie 2: Cryptographie moderne

* par bloc

* par flux

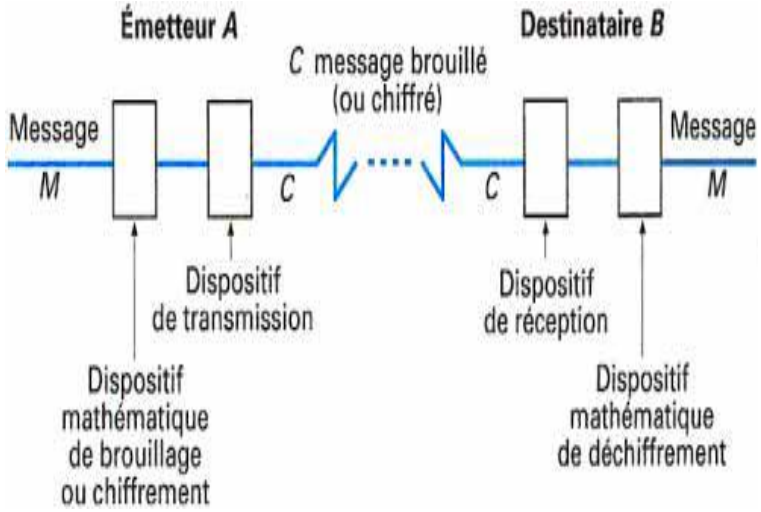
Chapitre 4: Gestion des clés et fonction de hashage

Chapitre 1 : Introduction

Problématique et Objectif ?

Depuis longtemps, les êtres humains ont tenté de rendre sécuritaires leurs communications confidentielles.
Différentes techniques ont été utilisées.

Stéganographie



FAGEMYREMPURZV_EMZR_R FMNMDAZR

Cryptographie

Problématique ?

L'image contient un message secret (message caché ou une image ou même un son)

a) Stéganographie

Message incompréhensible

FAGEMYREMPURZV_EMZR_R FMNMDAZR

b) Cryptographie

Introduction

Au début, il s'agissait seulement de cacher l'existence du message. Cette technique s'appelle la **stéganographie.**

Puis, des techniques de plus en plus sophistiquées furent utilisées pour rendre les messages compréhensibles seulement par leurs destinataires **légitimes**. (**Cryptographie**)

Tout au cours de l'histoire, une difficile bataille eut lieu entre les *constructeurs* de code (**cryptographes**) et ceux qui essayaient de les *briser* ou casser (les **cryptanalystes**).

Il n'est toujours pas clair, même aujourd'hui, qui sera le **vainqueur.**

La Stéganographie

Introduction à la stéganographie

- La stéganographie est l'art de "cacher" une information privée ou secrète dans un support.
- Plusieurs techniques ont été utilisées:
- Deux types de stéganographie:
  - Classique
  - Moderne

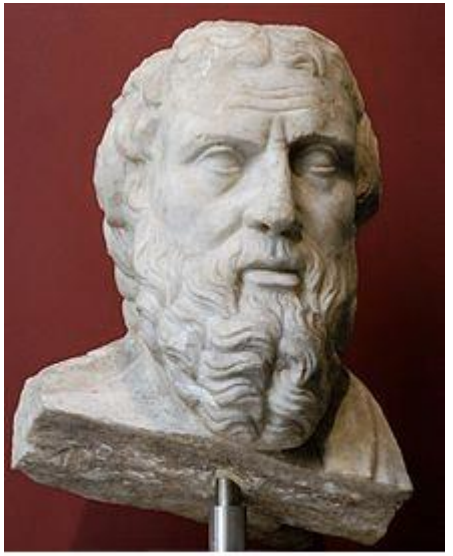
A) Stéganographie classique

Le plus ancien exemple de stéganographie a été rapporté par Hérodote. C'était lors du conflit entre la Grèce et la Perse(Iran) au 5ième siècle avant. Jessis-Crist.

1- Les Perses voulaient conquérir la Grèce et avaient préparé pendant 5 années une imposante armée. Heureusement pour les Grecques, Damaratus, un Grec exilé en Perse eu vent de ce projet.

Il inscrivit son message sur des tablettes de bois et les recouvrit de cire. Les tablettes avaient donc l'air vierges. Elles n'attirèrent pas l'attention des gardes tout au long du parcours.

Les Grecques, une fois mis au courant de l'attaque perse à venir, eurent le temps de se préparer et lors de l'attaque, ils mirent l'armé perse en déroute.



Hérodote

Stéganographie

2- Hérodote rapporte aussi l'histoire d'Histaïaeus qui, pour transmettre un message, rasa la tête de son messager et inscrivit le message sur son crane. Une fois les cheveux repoussés, le messager put circuler sans attirer l'attention.

3- Durant la Deuxième Guerre mondiale, les Allemands utilisaient la technique du micropoint. Il s'agit de photographier avec un microfilm le document à transmettre. La taille du microfilm était de moins d'un millimètre de diamètre. On plaçait le micropoint à la place du point final d'une lettre.

En 1941, le FBI repéra le premier micropoint. De nombreux messages furent par la suite interceptés.

Stéganographie

4- Écritures dissimulées

l'utilisation d'encres sympathiques, (premier siècle avant J.-C.) On écrit, au milieu des textes écrits à l'encre, un message à l'aide de jus de citron, de lait, de certains produits chimiques. Il est invisible à l'oeil, mais une simple flamme, ou un bain dans un réactif chimique, révèle le message

Stéganographie

5- Une autre méthode très répandue de stéganographie est de dissimuler le message dans le texte lui-même (Stéganographie linguistique)

- **Message 1 en clair:**

  VERONIQUE

- Message codé:

  dans la béatitude à perpétuité
  dans la félicité toujours
  en paradis irrévocablement
  dans la déité dans la béatitude
  à perpétuité

- **Message 2 en clair:**
- CRYPTOGRAPHIE :

A = dans les cieux	N = en paradis
B = à tout jamais	O = toujours
C = un monde sans fin	P = dans la divinité
	Q = dans la déité
D = en une infinité	R = dans la félicité
E = à perpétuité	S = dans son règne
F = sempiternel	T = dans son royaume
G = durable	U-V-W = dans la béatitude
H = sans cesse	
I-J = irrévocablement	X = dans la magnificence
K = éternellement	
L = dans la gloire	Y = au trône
M = dans la lumière	Z = en toute éternité

un monde sans fin dans la félicité au trône dans la divinité dans son royaume toujours durable dans la félicité dans les cieux dans la divinité sans cesse irrévocablement à perpétuité

Stéganographie

6- La Seconde Guerre Mondiale a vu de nombreuses formes de stéganographie. Les méthodes étaient parfois assez rudimentaires, comme ce message envoyé par un espion allemand :

Apparently neutral's protest is thoroughly discounted and ignored. Ismam hard hit. Blockade issue affects pretext for embargo on by-products, ejecting suets and vegetable oils.	Apparemment la protestation des pays neutres est totalement ignorée. Isman frappe fort. L'issue du blocus donne des prétextes pour un embargo sur certains produits, mis à part graisses animales et huiles végétales.

Cela semble tout à fait normal. Maintenant, en prenant la deuxième lettre de chaque mot, on obtient : **Pershing sails from NY June 1** (le Pershing part de New-York le 1er juin)

Stéganographie

7-

a)Différentes méthodes linguistiques existent également. Pour cacher un message dans un texte, on peut jouer sur l'espace entre les mots, la ponctuation, ou encore l'orthographe. A l'origine, c'est l'acrostiche qui permettait de cacher ces messages. L'acrostiche est un poème dont la première lettre de chaque vers compose un mot ou une phrase.

b)La ponctuation permit aussi d'identifier certains messages cachés. Au XV IIe siècle, Sir John Trevanion fut arrêté et emprisonné dans un chateau. Il reçu alors une lettre, que les gardiens avaient jugés sans danger. Lorsque John lut celle-ci, il détecta la présence suspecte de certaines virgules étrangement placées. Il repéra également qu'en prenant la troisième lettre de chaque mot suivant ces virgules, il pouvait former le message

Stéganographie

8- Un moyen de communication assez complexe mais parfaitement efficace était donné par la dissimulation d'un court message dans une lettre ordinaire selon le "Barn Code". Nous donnons un exemple détaillé; supposons que l'agent reçoit par la poste la lettre ci-après:

Mon cher Pierre,

J'espère que tu voudras bien m'excuser, mais j'ai eu tellement de travail à la maison que je n'ai pas pris le temps d'écrire aux amis. Cependant je t'envoie ce petit mot d'urgence pour te faire savoir que si tu veux des pneus, tu ferais bien de te dépêcher; en effet:

Hier, Jean est venu nous rendre visite, il descendait du train et s'est arrêté un moment chez nous pour bavarder et donner des nouvelles à mon père de son Paris. En principe, il doit rester quelques jours ici pour mettre en ordre ses affaires avant de repartir pour la capitale. A Paris, c'est calme, mais la veille il avait été dérangé en plein sommeil par les sirènes deux fois dans la nuit! Ceci mis à part, il doit nous faire envoyer par un ami à lui des pneus neufs pour nos vélos. Il en a pour le moment, profitons-en! A bientôt de tes nouvelles.

Stéganographie

Extrayons le dixième mot du premier paragraphe: "Tellement" et disposons-le comme une clef avec son équivalence numérique. Écrivons ensuite le second paragraphe de la lettre sous cette clef.

T	E	L	L	E	M	E	N	T
8	1	4	5	2	6	3	7	9
Hier,	**Jean**	est	venu	nous	rendre	visite,	il	descendait
du	train	et	s'est	**arrêté**	un	moment	chez	nous
pour	bavarder	et	donner	des	nouvelles	**à**	mon	père
de	son	**Paris**.	En	principe,	il	doit	rester	quelques
jours	ici	pour	**mettre**	en	ordre	ses	affaires	avant
de	repartir	pour	la	capitale.	**A**	Paris,	c'est	calme,
mais	la	veille	il	avait	été	dérangé	**en**	plein
sommeil	par	les	sirènes	deux	fois	dans	la	nuit!
Ceci	mis	à	part,	il	doit	nous	faire	**envoyer**
par	**un**	ami	à	lui	des	pneus	neufs	pour
nos	vélos.	Il	en	**a**	pour	le	moment	profitons-
en!	A	bientôt	de	tes	nouvelles.			

Le texte apparaît lu horizontalement, un mot par ligne, sous les colonnes repérées dans l'ordre numérique de la clé:
"Jean arrêté à Paris. Mettre *a* en sommeil. Envoyer un *a*."

B) Stéganographie moderne

- Avec le développement de l'informatique: la multiplication des transferts de fichiers sur les réseaux, la stéganographie est devenue un sujet à la mode avec de nombreuses innovations.
- Il est facile, en effet, de glisser quelques bits discrets au milieu d'un flot d'images, de textes ou de programmes.
- Les moyens de cacher sont innombrables, des plus rudimentaires(simples) aux plus sophistiqués(difficiles):

B) Stéganographie moderne

Quelques techniques de stéganographie appliquées à l'image et au son.

1- La Méthode LSB (Least Significant Bit), ou méthode de bit de poids faible

2- Technique de Dissimulation d'information dans une image:

Le Watermarking(tatouage)

3 - Cacher une image dans une autre image

4- Cacher du texte dans une image

5- Message caché dans un Son

6- Sécurité

7- la stéganalyse

Des notions sur l'image numérique

Le pixel : Ç'est la plus petite unité affichable à l'écran. Un pixel est constitué de 3 octets : un octet pour la composante rouge, un octet pour la composante verte et un octet pour la composante bleue. C'est pour cela que l'on parle de RVB (Rouge Vert Bleu).

*A partir de ces trois octets, on peut donc avoir 256*256*256 = 16777216 (16 millions) de couleurs différentes, ce qui est largement plus que ne peut distinguer l'oeil humain.*

L'image : Ce n'est ni plus ni moins que le stockage dans un fichier de tous les pixels RVB composant l'image finale. Par exemple, une image 800×600 pixels correspond à 800x600x3 = 1440000 octets.

Des notions sur l'image numérique

La définition est le nombre de points (ou pixels) que comporte une image numérique en largeur et en hauteur. On l'exprime en donnant le nombre de pixels en hauteur et en largeur (exemple : 1600x1200).

La résolution est le nombre de pixels par unité de longueur. La résolution est exprimée le plus souvent en ppp (point par pouces) ou en dpi (dots per inch). Rappel : 1 pouce = 2.54 cm.

Une image de 100 ppp (ou 100 dpi) contient 10 000 points par pouce carré. (100 x 100 = 10 000)

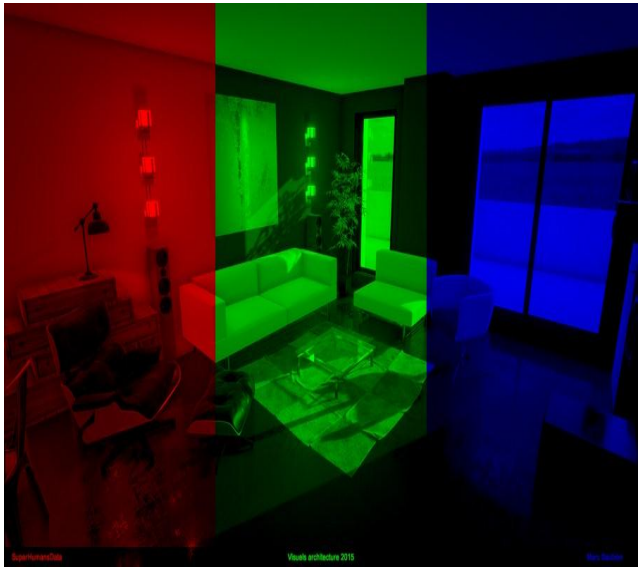
La résolution définit la netteté d'une image et sa qualité d'affichage à l'écran. Plus la résolution est grande (c'est-à-dire plus il y a de pixels dans une longueur de 1 pouce), plus votre image est précise dans les détails.

Des notions sur l'image numérique

Formats des images: BMP(bitmap), JPEG, JIFF, PNG; TIFF

Mode RVB et CMJN

Les données de l'image sont conservées sur différentes couches, rouge, vert et bleu pour le RVB ou cyan, magenta, jaune et noir pour le CM



Etude du format BMP (bitmap)

Chaque format graphique renferme des informations multiples identifiables par l'analyse des octets qu'il renferme(entete).

Contenu du fichier

La première partie appelée **ENTETE DU FICHIER** (file header) est composé de quatre champs sur 14 octets :

- La signature (sur 2 octets) :BM, 424D en hexadécimal pour signifier qu'il s'agit d'un fichier BMP.
- La taille totale du fichier en octets (codée sur 4 octets)
- Un champ réservé (sur 4 octets)
- Le décalage de l'image (sur 4 octets), qui donne l'adresse relative du début des données qui concernent l'image

Des notions sur l'image numérique

La deuxième partie est **l'ENTETE DE L'IMAGE** (information Header) qui informe comme son nom l'indique sur l'image sur 4 champs de 40 octets :

La taille de l'entête de l'image en octets (codée sur 4 octets).

La largeur de l'image (sur 4 octets),

La hauteur de l'image (sur 4 octets),

Le nombre de plans (sur 2 octets).

La profondeur de codage de la couleur (sur 2 octets)

La méthode de compression (sur 4 octets).

La taille totale de l'image en octets (sur 4 octets).

La résolution horizontale (sur 4 octets),

La résolution verticale (sur 4 octets),

Le nombre de couleurs de la palette (sur 4 octets)

Le nombre de couleurs importantes de la palette (sur 4 octets).

Des notions sur l'image numérique

La troisième partie représente l'image avec le CODAGE de chaque pixel ligne par ligne. Le codage de l'image se fait en écrivant successivement les bits correspondant à chaque pixel, ligne par ligne en commençant par le pixel **en bas à gauche**.

1. Les images en 2 couleurs utilisent 1 bit par pixel, ce qui signifie qu'un octet permet de coder 8 pixels
2. Les images en 16 couleurs utilisent 4 bits par pixel, ce qui signifie qu'un octet permet de coder 2 pixels
3. Les images en 256 couleurs utilisent 8 bits par pixel, ce qui signifie qu'un octet code chaque pixel
4. Les images en couleurs réelles utilisent 24 bits par pixel, ce qui signifie qu'il faut 3 octets pour coder chaque pixel, en prenant soin de respecter l'ordre de l'alternance bleu, vert et rouge.

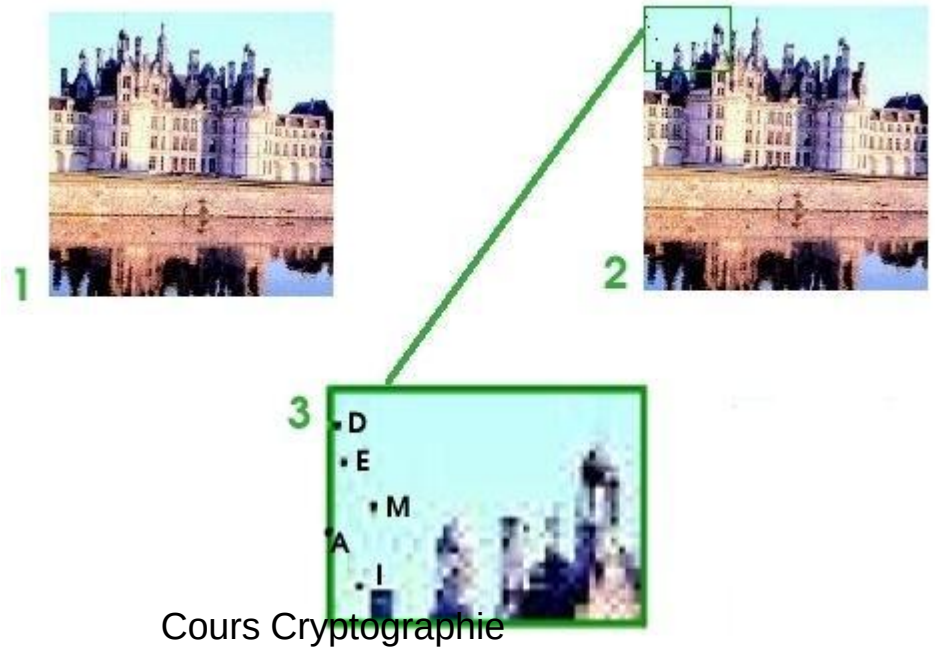
Les techniques:

1- Cacher une information dans une l'image

- L'astuce est d'utiliser un bit à chaque octet RVB qui compose chaque pixel de l'image. En effet, en retirant 1 bit, on dégrade l'image, mais ce n'est pas visible à l'oeil nu. On peut récupérer ce bit à chaque fois et l'utiliser pour stocker les données que l'on souhaite.

1- Cacher une information dans une l'image

- Nous récupérons donc 1/8e de la taille de l'image pour cacher une information ou un document. Dans notre exemple, une image 800×600 pixels permet de stocker une information de 180000 octets.
- Cela peut être, par exemple, pour stocker un document Word (3 pages de texte) à l'intérieur de l'image…soit sur toute l'image ou dans une zone de l'image



2- Une Technique de Dissimulation d'information dans une image : Le Watermarking(Tatouage numérique)

- Il s'agit d'une technique pour protéger les images numériques, en insérant une signature à l'intérieur des images numériques sur Internet, afin de lutter contre la fraude et le piratage et d'assurer la protection des droits de propriété intellectuelle. Ainsi, en cas de litige de droits d'auteurs, le watermark sera montré pour prouver l'originalité de l'oeuvre.

2- Une Technique de Dissimulation d'information dans une image : Le Watermarking(Tatouage numérique)

- On distingue deux classes de tatouage: visibles et invisibles.
- Les visibles altèrent le signal ou le fichier (par exemple ajout d'une image pour en marquer une autre).
- Les invisibles: la stéganographie

2- Une Technique de Dissimulation d'information dans une image : Le Watermarking(Tatouage numérique)

- On distingue deux **types d'attaques**, celles **passives** et celles **actives**. Les premières visent simplement à détecter la présence d'un tatouage invisible caché dans l'image.
- Les secondes attaques cherchent à éliminer cette marque.

3- La Méthode LSB (Least Significant Bit), ou méthode de bit de poids faible

Méthode consiste à modifier les bits de poids faibles des pixels codant l'image.

Une image est un tableau constitué d'un ensemble de pixels.

Pour chaque pixel, on code la couleur avec trois octets : un pour le rouge, un pour le vert, un pour le bleu.

Chaque octet indique l'intensité de la couleur correspondante, sur un niveau allant de 0 à 255.

255 correspond à la couleur native. Passer d'un niveau N à un niveau N – n, où n est suffisamment petit ne modifie que de peu la couleur , et c'est précisément sur cela que repose la méthode LSB.

Mise en pratique :

On prend un octet correspondant à l'une des trois couleurs d'un pixel, par exemple 01101011.

Si on change les quatre derniers bits, cela ne change que de peu la couleur.

Dans notre exemple, 0110**1011**, **1011** correspond donc aux bits de poids faible.

L'idée est de remplacer ces bits de poids faible par ceux de l'information que l'on souhaite dissimuler(cacher).

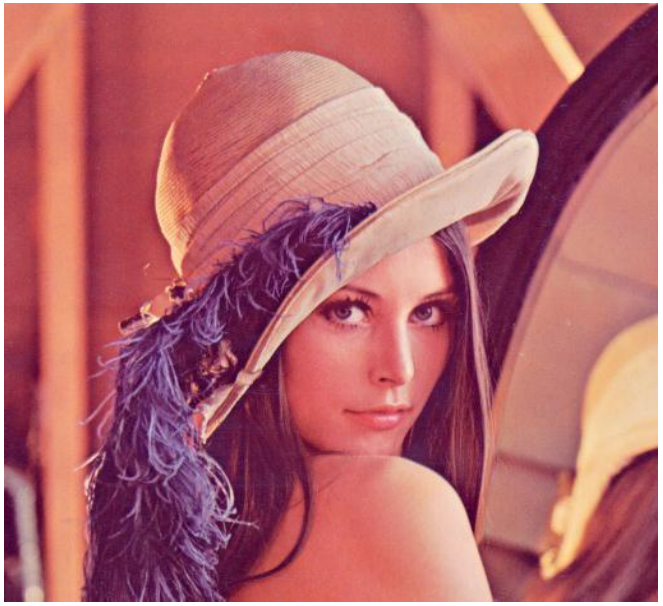
4- Cacher une image dans une autre

- Soit un octet de l'image qui cache 01101011 et un octet de l'image que l'on souhaite cacher 10011101.
- Le but est de remplacer les bits de **poids faible** de l'image qui cache par les bits de **poids fort** de l'image qu'on souhaite cacher.
- Ainsi, on obtiendra l'octet 01101001. Attention, on effectue des changements sur des détails. Il faut choisir une image qui cache qui présente suffisamment de changements, auquel cas l'image cachée s'apercevra.

4-Cacher une image dans une autre

Prenons comme image qui cache une autre image:

Et comme image à dissimuler (cacher):



4-Cacher une image dans une autre


```
s=cacher_im3(lena, rue)
imwrite(s,'lena1.tif','tif')
```

En sortie, on obtient l'image :

Maintenant retrouvons notre rue

```
[s1,s2]=trouver_im3(lena1)
imwrite(s2,'rue2.tif','tif')
```

s1 et s2 correspondent respectivement à l'image qui cache et l'image cachée, qui, au passage, n'ont plus leur bits de poids faible.

Il me reste juste à afficher s2 :

On retrouve bien notre homme à vélo

5- Message caché dans un Son

De faibles variations, imperceptible pour l'oreille, dans les basses fréquences ou ce que l'on appelle le bruit de fond peuvent contenir une grande quantité d'information.

Afin de rester indécelable, le bruit artificiel doit posséder les propriétés statistiques d'un vrai bruit de fond.

On ajoute le texte à cacher dans la partie bruit du son,

6- Sécurité par compression

On pose la question : pourquoi vouloir dissimuler une information si l'on a rien à se reprocher? Cela soulève la question de la sécurité.

Un employé mal intentionné peut, par exemple, vouloir faire sortir d'une entreprise des données confidentielles. Il existe toutefois un moyen simple pour contrecarrer cela.

On travaille sur des images qui ne sont pas compressées. Si l'on compresse l'image dans un format destructif comme le JPEG, l'information dissimulée va être altérée.

Si on effectue une opération de compression décompression à toutes les images qui sortent de l'entreprise on détruit notre message.

On parle alors de **stérilisation.**

7- Avantages et inconvénients du LSB

L'avantages du LSB:

- La taille du fichier n'est pas modifiée, puisque le message est encodé dans les parties peu ou pas utilisées du fichier.
- Méthode rapide et facile à mettre en œuvre.

Inconvénients du LSB:

la perte du message lorsque des changements importants ont lieu sur le support, comme par exemple une rotation, ou un redimensionnement de l'image

Amélioration:

Une amélioration du LSB consiste à introduire un paramètre aléatoire permettant de distribuer les bits de poids faible utilité.

Les modifications n'auront pas lieu "uniquement" dans les premiers octets de l'image, mais seront au contraire répartis aléatoirement dans l'entièreté de l'image.

8-Les limites de la stéganographie , watermarking

La dissimulation d'information dans un document porteur est fortement dépendant de la nature de ce document porteur.

Par exemple, une information dissimulée dans une image BMP est détruite si l'image est convertie en JPG.

En effet, le JPG comporte son propre algorithme de compression qui dégrade volontairement l'image afin d'obtenir un compactage maximum.

Les précieux bits de l'information cachée sont donc fortement altérés par le compactage.

9- La stéganalyse

La stéganalyse consiste à identifier la présence d'un message. Le message lui-même pourra être retrouvé, mais ce n'est pas l'objectif principal de la stéganalyse.

Il existe deux catégories d'attaques:

1-Les attaques passives : Identifier la présence d'un message, dans le but secondaire de pouvoir le reconstituer par la suite. Peuvent prendre plusieurs formes :

- la lecture ou l'écoute du fichier,
- la comparaison avec le fichier original (si il est disponible),
- certaines attaques statistiques (attaques sur le LSB),

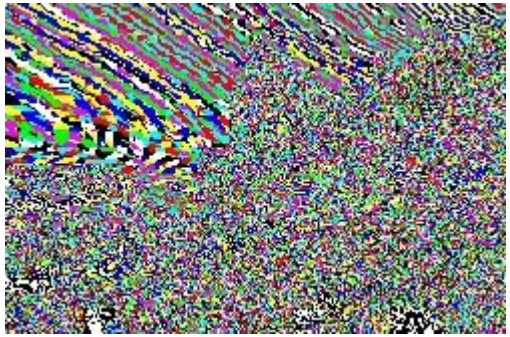
2-Les attaques actives : elles consistent à détruire le message caché, sans prêter attention à ce qu'il signifie. L'objectif est de supprimer le message, ou en tout cas, à le rendre inutilisable.

Cette destruction aura souvent lieu par l'intermédiaire de modifications du support (redimensionnement (image, vidéo), filtrage (sons), compression, ...).

La stéganalyse

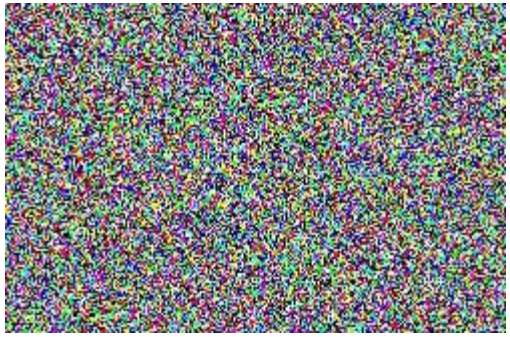
1- Analyse des couleurs obtenues en ne gardant que les bits de poids faibles,

Image initiale



Couleurs obtenues en ne gardant
que les bits de poids faible

Image modifiée



Couleurs obtenues en ne gardant
que les bits de poids faible

2- Analyse statistiques

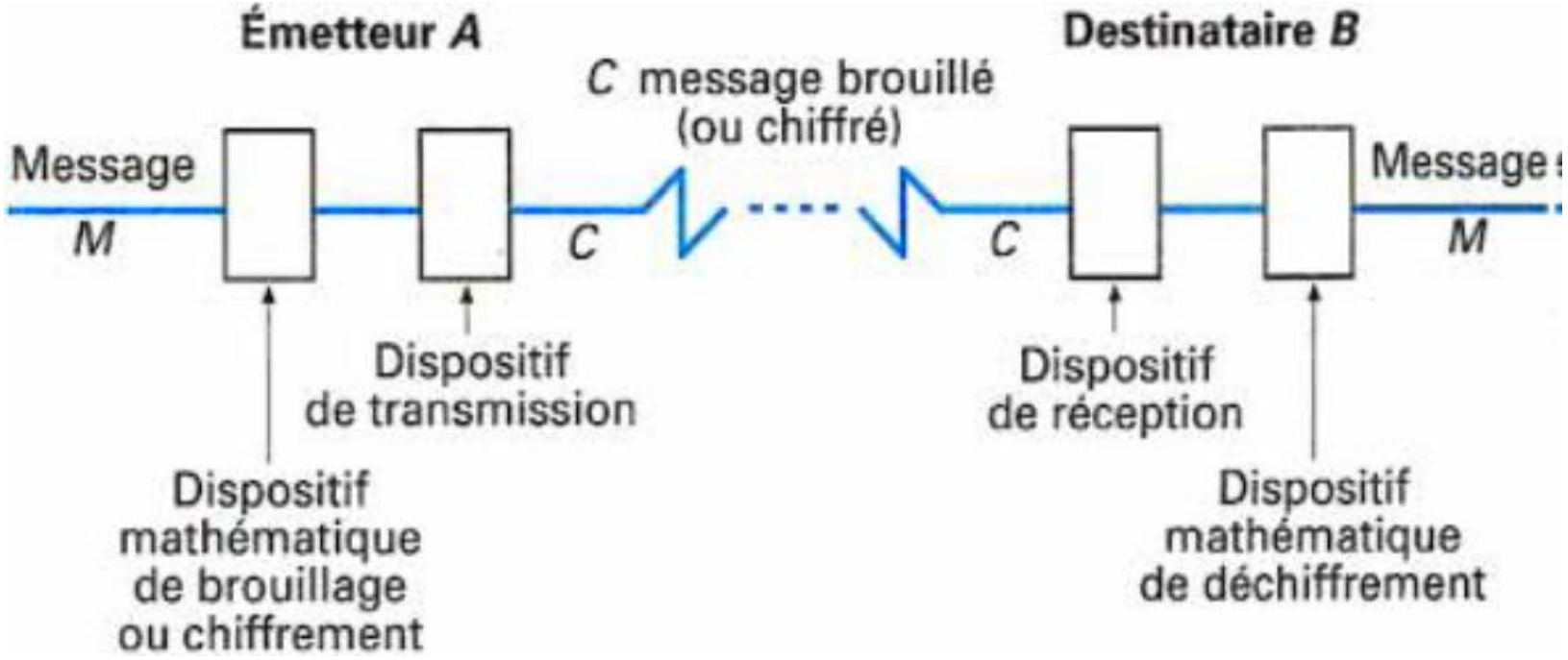
La Cryptographie

C) Les quatre buts(objectifs) de la cryptographie

- **Confidentialité** : mécanisme pour transmettre des données de telle sorte que seul le destinataire autorisé puisse les lire.
- **Intégrité** : mécanisme pour s'assurer que les données reçues n'ont pas été modifiées durant la transmission.
- **Authentification** : mécanisme pour permettre d'identifier des personnes ou des entités et de certifier cette identité.
- **Non-répudiation** : mécanisme pour enregistrer un acte ou un engagement d'une personne ou d'une entité de telle sorte que celle-ci ne puisse pas nier avoir accompli cet acte ou pris cet engagement. (traçabilité)

D) Définition de la cryptographie

- Science **mathématique** permettant d'effectuer des opérations sur un texte **intelligible(simple)** afin d'assurer une ou plusieurs propriétés de la sécurité de l'information.



1- Utilisation de la cryptographie(domaine d'application)

Armée (sécurité)
Système bancaire,
Internet (achats, identification, déclaration d'impôts),
Téléphones portables,
clefs électroniques (e.g., voitures)
TV payante,
Cartes d'identités électroniques,
cartes de santé,
Vote électronique,
DVD, HD DVD, Blue Ray, audio numérique (certains formats, e.g., WMA, AAC),
Consoles de jeux vidéos (e.g., Xbox, Xbox360).

La cryptographie est partout !!

Où trouver de la cryptographie ?

- Armée (sécurité)
- Système bancaire,
- Navigateurs web : Mozilla Firefox ou Internet Explorer,
- Internet (achats, identification, déclaration d'impôts),
- Téléphones portables,
- Clefs électroniques (e.g., voitures)
- TV payante,
- Cartes d'identités électroniques,
- Cartes de santé,
- Vote électronique,
- Consoles de jeux vidéos (e.g., Xbox, Xbox360).

2- Principes fondamentaux et terminologie

1) Vocabulaire:

- **Cryptologie:** est une science mathématique qui comporte deux branches: la cryptographie et la cryptanalyse.
- **Cryptographie :** science qui utilise les mathématiques pour le cryptage et le décryptage de données.
  - C'est aussi l'étude des techniques mathématiques en rapport avec les aspects de la sécurité informatique (confidentialité, intégrité et authenticité)
- **Cryptanalyse :** c'est l'étude des informations cryptées, afin d'en découvrir le secret. Les Cryptanalystes sont également appelés des « pirates ».

- *La **cryptographie** est la science qui consiste à écrire l' information (voix, son, textes, image fixe ou animée) en la rendant incompressible à ceux ne possédant pas les capacités de la déchiffrer.*
- *La **cryptanalyse** est l'ensemble des moyens qui permettent d'analyser une information chiffrée, afin de la déchiffrer.*

2-Principes fondamentaux et terminologie

1) Vocabulaire:

- **Le chiffrement** est l'opération par laquelle on crypte un message, c'est une opération de codage.
- **Chiffrer** ou **crypter** une information a pour but de la rendre incompressible en l'absence d'un décodeur particulier.
- Cryptage (chiffrement): méthode permettant de dissimuler le texte en clair en masquant son contenu. Cette opération permet s'assurer que seules les personnes auxquelles les infos. Sont destinées pourront y accéder.

- un **cryptogramme** est un message écrit en langage chiffré (message chiffré).
- **Texte en clair (Plaintext):** données lisibles et compréhensible sans intervention spécifique.
- **Texte chiffré** (**Ciphertext**): texte inintelligible résultant du cryptage.
- **Décryptage** (déchiffrement): processus inverse de transformation du texte chiffré en texte clair.

2) Algorithmes et clés des chiffrement

- Les systèmes de chiffrement utilisent des **algorithmes de chiffrement** qui s'appuient sur des fonctions mathématiques souvent complexes qui, à l' aide d' une **clé de chiffrement**, modifient les données à protéger en générant des données apparemment aléatoires.
- Le texte chiffré (cyphertext) peut alors être envoyé sur un réseau **non sécurisé**.
- Même s' il est intercepté, le cryptogramme, est uniquement compréhensible par un **tiers** qui possède la clé de déchiffrement permettant d' obtenir le texte initial en clair(plaintext).

Pour une vraie sécurité, tous les algorithmes modernes utilise une clé. Cette clé peut prendre une des valeurs parmi un grand nombre de valeurs possible (espace des clés)

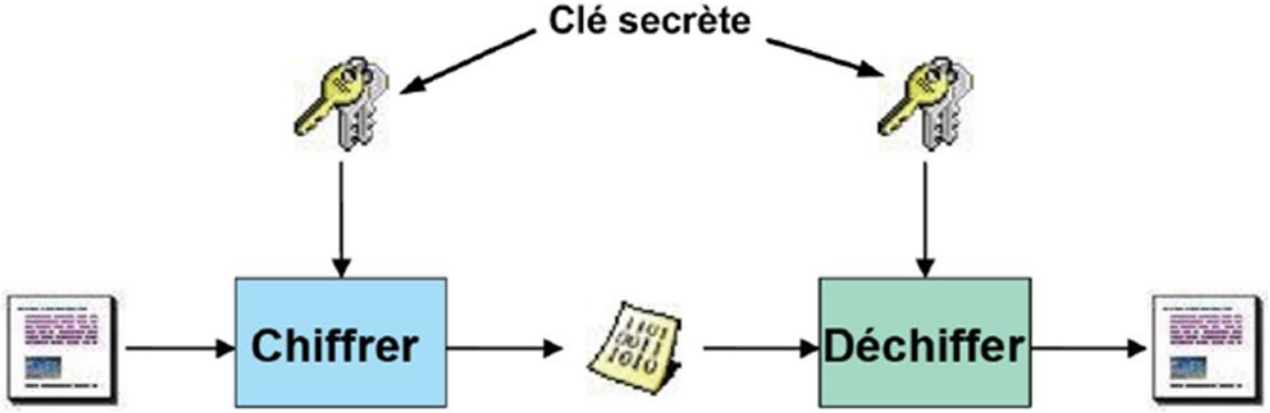
- La valeur de la clé « K » **affecte** les algorithmes de chiffrement et de déchiffrement, et donc les fonctions correspondantes « e_K » et « d_K »

2) Algorithmes et clés des chiffrement

a) Cryptographie de clé secrète (symétrique)

Les deux entités partagent une clé secrète

La clé sert au chiffrement et au déchiffrement



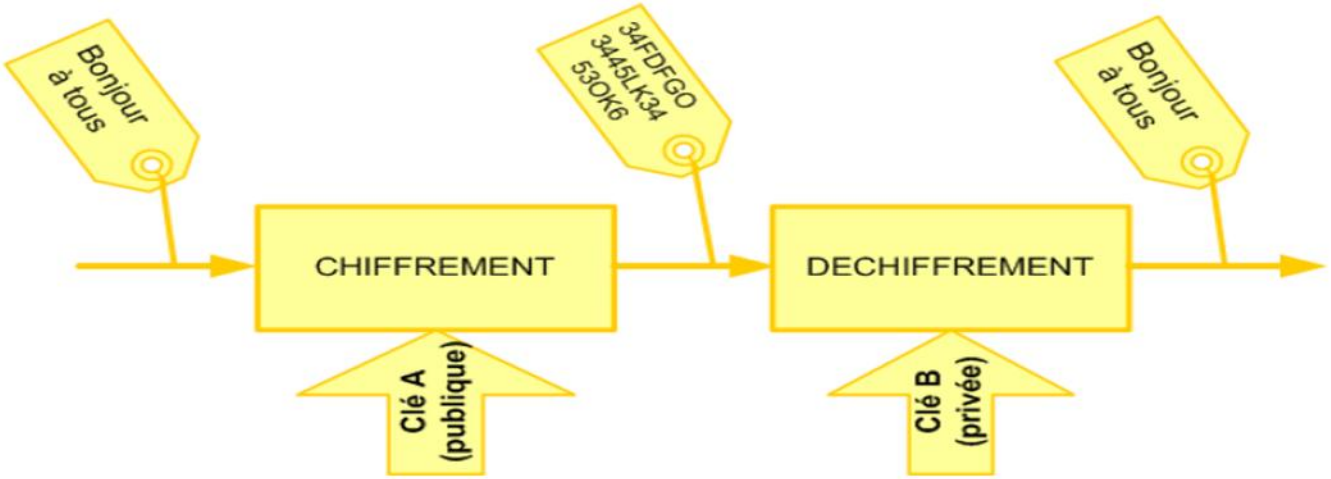
- Dans ce cas, pour un message « m », on écrit

$$e_K(m) = c,\ d_K(c) = m \quad \text{et} \quad d_K(e_K(m)) = m$$

2) Algorithmes et clés des chiffrement

b) Cryptographie de clé asymétrique

- Une clé publique diffusée à tout le monde, utilisée pour chiffrer le message.
- Une clé privée tenue secrète, utilisée pour déchiffrer le message.



- Dans ce cas, on écrit :

$$e_{K1}(m) = c,\ d_{K2}(c) = m \ \text{ et } \ d_{K2}(e_{K1}(m)) = m$$

- **Cryptosystème** : Il est défini comme l'ensemble des clés possibles (espace de clés), des textes clairs et chiffrés possibles associés à un algorithme donné.
- quintuplet $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$, tel que :
  - $\mathcal{P}$: ensemble de textes en clair
  - $\mathcal{C}$: ensemble fini de textes chiffrés
  - $\mathcal{K}$: espace de clés
  - Pour chaque $K \in \mathcal{K}$, il y a une fonction de cryptage $e_K \in \mathcal{E}$, et une fonction de décryptage correspondante $d_K \in \mathcal{D}$, tel que

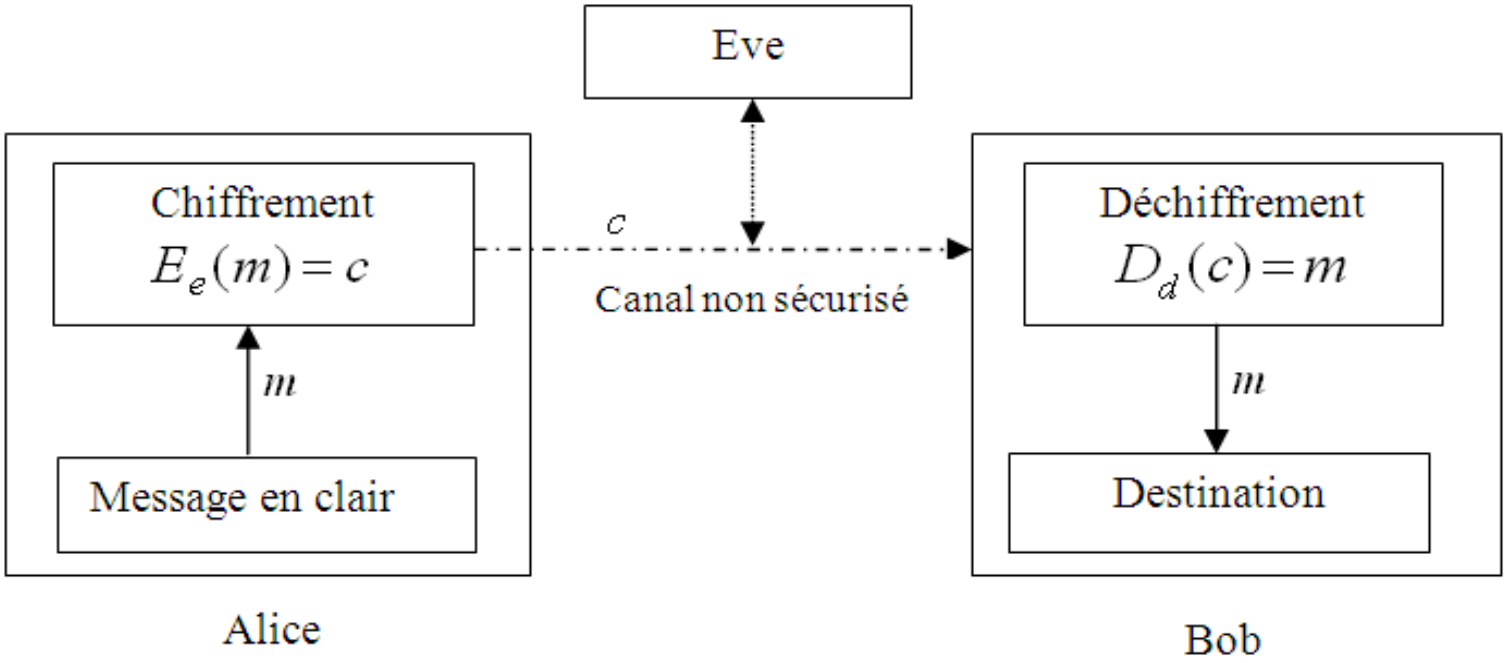
$$d_K(e_K(x)) = x, \text{ pour tout } x \in \mathcal{P}$$

Principe de Kerckhoff ?

La sécurité du chiffre ne doit pas dépendre de ce qui ne peut pas être facilement changé.

En d'autres termes, aucun secret ne doit résider dans l'algorithme mais plutôt dans la clé. Sans celle-ci, il doit être impossible de retrouver le texte clair à partir du texte chiffré. Par contre, si on connaît K, le déchiffrement est immédiat.

- Deux participants en communication dans un modèle de chiffrement.



e est la clé de chiffrement.

d est la clé de déchiffrement.

E, D sont les algorithme du chiffrement et du déchiffrement.

Eve joue le rôle d'un attaquant

3) Taille de la clé

- Une clé codée sur n bits (**taille de la clé**) peut prendre 2^n valeurs. Plus la clé est longue, plus le nombre de clés possibles est important, et plus cela nécessite de la **puissance et du temps de calcul** (pour un attaquant) pour le trouver.
- Une clé de chiffrement/déchiffrement doit avoir **une taille minimale** afin d' éviter qu'elle soit déterminée trop facilement.

3)Taille de la clé

- Il est devenu relativement simple de casser des clés d' une longueur de 40 bits (environ 10^{12} possibilités de clés différentes), il est préférable de chiffrer les informations sensibles avec des clés plus longues de 128 bits (10^{38} possibilités) ou 256 bits, par exemple.
- Casser de telles clés demande une très lourde infrastructure informatique et des temps de traitement important, ce qui est un empêchement pour certains(amateurs).
- ➔
- **Le moyen le plus simple pour obtenir une clé est de la procurer directement auprès de l'utilisateur ou à partir du système qui la stocke, plutôt que d'essayer de la deviner par itération.**

4)Robustesse du système

- La taille de la clé utilisée, la puissance de l'algorithme et la capacité à garder les clés secrètes de façon sécurisée, déterminent **la robustesse** d'un système de chiffrement.
- **L'algorithme n'a pas besoin d'être secret**. Il est même recommandé qu'il soit publié afin que la communauté scientifique puisse tester sa résistance aux attaques et trouver les failles avant qu'un attaquant ne les exploite.
- Un système de chiffrement est dit **fiable, robuste, sûr ou sécurisé** s'il reste **inviolable** indépendamment de la puissance de calcul ou du temps dont dispose un attaquant.

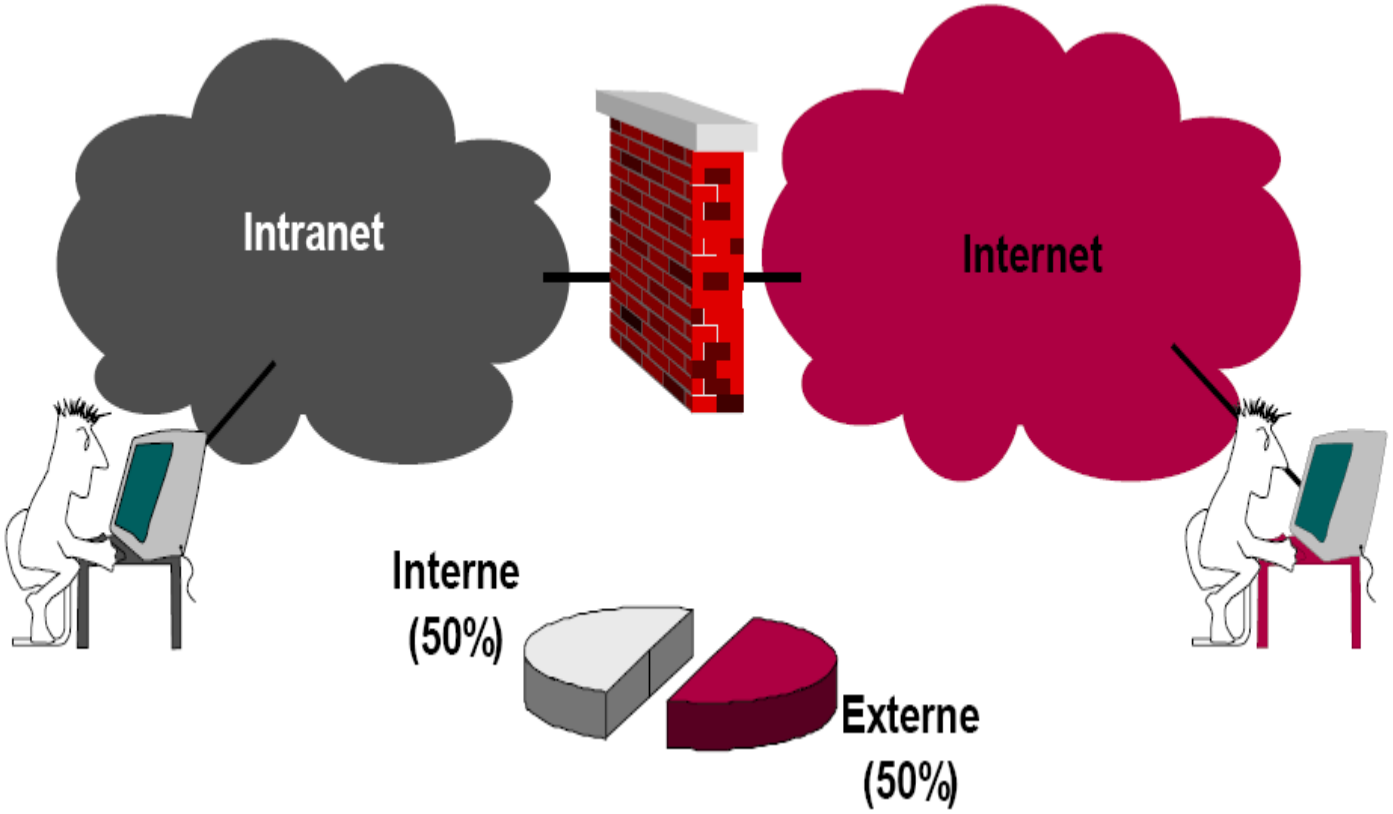
- **Remarques importantes:**

  - Plus une clé est spécifique et son utilisation est **limitée dans le temps**, voir à **usage unique**, meilleure est la sécurité du système de chiffrement.

  - La robustesse d' un système de chiffrement réside dans l'algorithme de chiffrement lui même et non sur la clé (l' algorithme est incassable), **modifier fréquemment les clés de chiffrement le rend encore plus sûr**.

  - Si l' algorithme constitue le maillon faible du système de chiffrement, changer la clé fréquemment n' augmente pas sa robustesse.

D ’ou viennent les attaques ?

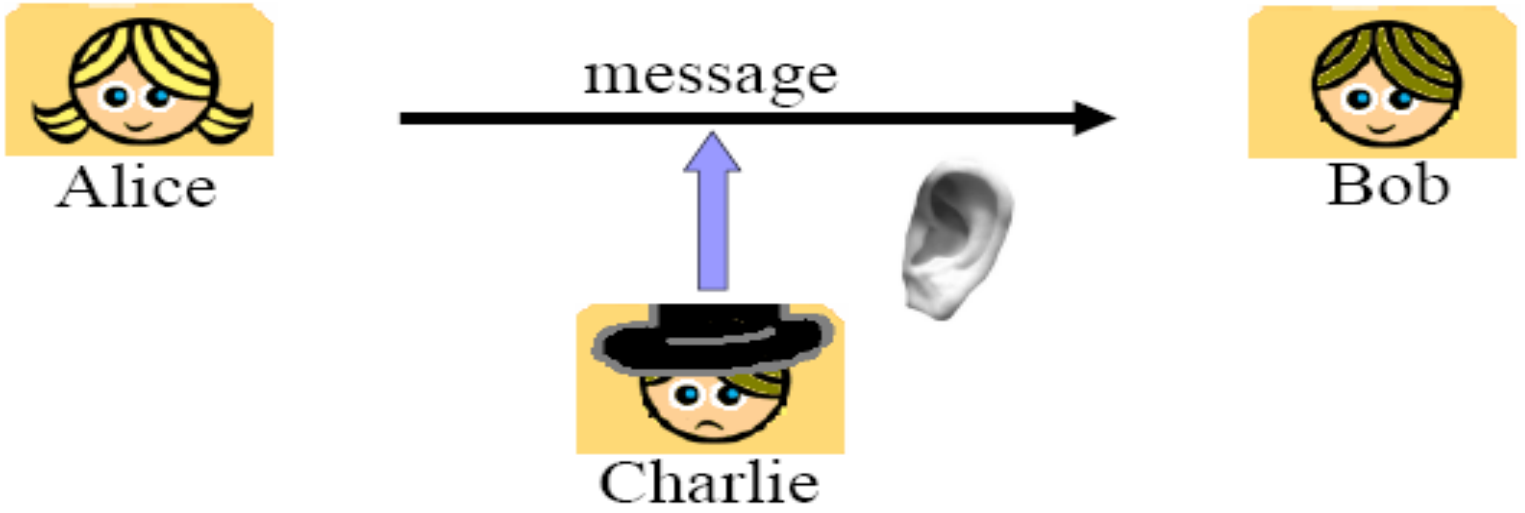


Les attaques ne viennent pas seulement de l’extérieur!

E) Types des attaques

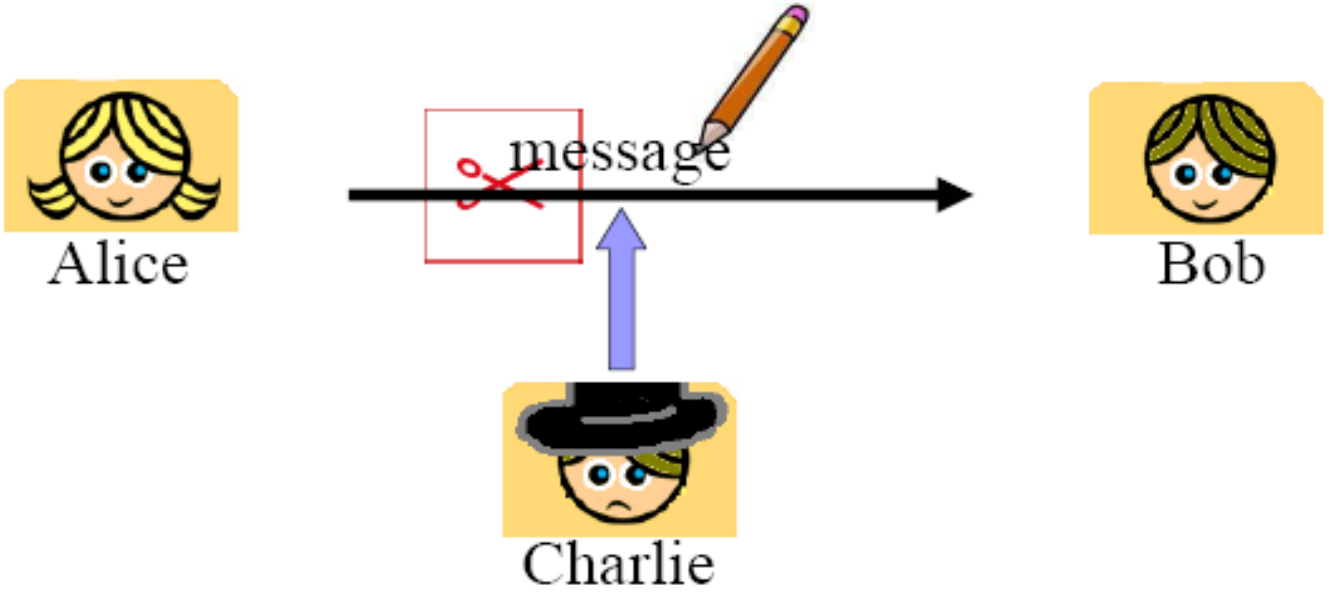
a-Attaques passives:

Menace contre la ***confidentialité*** de l'information : une information sensible parvient à une personne autre que son destinataire légitime. (entendre)



b-Attaques actives : interventions sur la ligne

Menace contre *l'intégrité et l'authenticité de l'information (modifier)*



Virus:

Un virus est un programme qui s'exécute sur un ordinateur et peut se répandre à travers d'autres machines d'un système d'une information dans l'objectif de provoquer des perturbations dans les applications informatiques.

1986 : le premier virus sort des laboratoires (Basit et Amjad Alvi)

Questions ?

Concepts mathématiques pour la cryptographie

1-Division entière

Diviseur:

Soient a, b et m $\in$ N. **a** divise **b** si $b = a\,m$

ou encore **a** est un diviseur de **b** et on note **a|b**.

Exemples:

les diviseurs de 24 sont: 1,2,3,4,6,8,12,24.

15 = 5 *3 donc:

3 divise 15

3 est un diviseur de 15

15 est un multiple de 3.

Ceci se note 3|15

1-Division entière

Propriétés:

Si a|1 alors a = ±1

Si a|b et b|a alors a = ±b

Tout b différent de 0 divise 0

Si a|b alors a|bc

Si a|b et b|c alors a|c

Si a|b et a|c alors a|b+c

Si a =0 mod n alors n|a

2-Test de divisibilité

- n est divisible par **2** s'il se termine par 0,2,4,6,8.

– n est divisible par **3** s'il a la somme de ses chiffres est divisible par3.

– n est divisible par **4** si ses deux derniers chiffres forment un multiple de 4 (ex:256628).

– n est divisible par **5** s'il se termine par 0 ou 5.

– n est divisible par **6** s'il est divisible à la fois par 2 ET par 3.

– n est divisible par **8** si ses 3 derniers chiffres forment un multiple de 8 (ex:176072).

2-Test de divisibilité (suite)

– n est divisible par **9** si la somme de ses chiffres est un multiple de 9 (ex: 37521=3+7+5+2+1=18=2*9).

– n est divisible par **10** si son dernier chiffre est 0.

– n est divisible par **11** si la différence (1er chiffre+ 3^{ième} chiffre+ 5^{ième} chiffre+...)-(2 ^{ième} chiffre + 4^{ième} chiffre+ 6^{ième} chiffre+...) est divisible par11.

Par exemple,1485 est divisible par11, car (1+8)-(4+5) = 0 est divisible par 11.

3-Exemple:

Question: Utiliser les tests de divisibilité pour déterminer si 216 est divisible par 2, 3, 4, 5, 6, 9 et 10.

216 est divisible par 2 puisque son dernier chiffre est 6.

216 est divisible par 3 puisque la somme de ses chiffres est 2+1+6 = 9, et 9 est divisible par 3.

216 est divisible par 4 puisque 16 est divisible par 4.

216 n'est pas divisible par 5 puisque son dernier chiffre n'est ni 5 ni 0.

Exemple(suite)

Question: Utiliser les tests de divisibilité pour déterminer si 216 est divisible par 2, 3, 4, 5, 6, 9 et 10.

216 est divisible par 6 puisqu'il est divisible à la fois par 2 ET par 3.

216 est divisible par 9 puisque la somme de ses chiffres est 9, et 9 est divisible par 9.

216 n'est pas divisible par 10 puisque son dernier chiffre n'est pas 0.

4-Algorithme de division ???

L'algorithme le plus simple consiste à soustraire autant de fois b de a qu'il est possible, jusqu' à obtenir un reste < b.

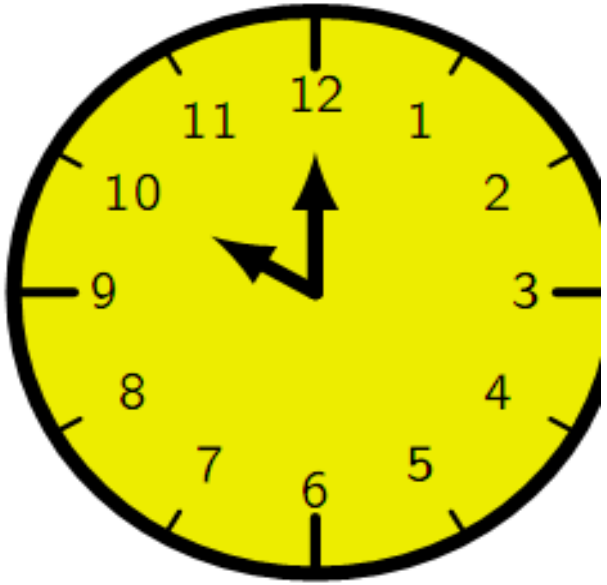
```
division:=proc(a,b)
local r, q, u ;

r := a ;
q := 0 ;
while (r >= b)
   do
     r := r − b ;
     q := q + 1 ;
  od ;
u := [q, r] ;
return(u) ;
end ;
```

5-Ensemble des entiers modulaires

Le "groupe de l'horloge"

- $2+5 = 7$
- $9+4 = 1$
- $8+12 = 8$
- $45+25 = 10 \mod 60\ldots$



Calcul "cyclique" ou *modulaire*

- 17h = 5h
- 0h17 + tous les 1/4 d'heure: 02, 17, 32, 47, 02,...

6-Congruence

Soit n, un entier non nul (dans Z), et a, b des entiers.

a et b sont dits congruents modulo n si
(a mod n)=(b mod n)
Ce qui s'écrit a = b mod n.

Exemples: 73 = 4 mod 23,

21 = -9 mod 10

Deux entiers a et b sont égaux (ou congrus) modulo n si **n|a-b**.

6-Congruence

Propriétés:

1. a = b mod n ssi n|a-b
2. a = b mod n ⇔ ca = cb mod (cn)
3. a = b mod n ⇔ ac = bc mod n
4. a = b mod m ⇔ b = a mod m
5. a = b mod n et b = c mod n → a = c mod n
6. ((a mod n)+(b mod n)) mod n =(a+b) mod n
7. ((a mod n)-(b mod n)) mod n =(a-b) mod n
8. ((a mod n)*(b mod n)) mod n =(a*b) mod n

Exemples

Propriété1: a = b mod n ssi n|a-b

23 = 8 (mod 5) car 23-8=15=5*3

-11 = 5 (mod 8) car -11 - 5= -16= 8*(-2)

Propriété 7:

((a mod n)-(b mod n)) mod n =(a-b) mod n

[(11mod 8)-(15 mod 8)] mod 8 = 3-7=(-4)mod 8 = 4

(11-15) mod 8 = (-4) mod 8 = 4

Propriété8:

((a mod n)*(b mod n)) mod n =(a*b) mod n

[(11 mod 8)*(15 mod 8)] mod 8 = (3*7) mod 8 = 5

(11*15) mod 8= 165 mod 8 = 5

7-Puissance

Il existe une autre technique pour la propriété n°8: la décomposition par facteurs plus simples.

Exemple: Pour trouver 11^7 mod 13, on peut procéder comme suit:

$11^2 = 121 \equiv 4 \pmod{13}$

$11^4 = (11^2)^2 \equiv 4^2 \equiv 3 \pmod{13}$

$11^7 \equiv 11 \times 4 \times 3 \equiv 132 \equiv 2 \pmod{13}$

Propriétés:

$a = b \bmod n$ et $c>0 \rightarrow a^c = b^c \bmod n$

$a = b \bmod n$ et ca et $b >0 \rightarrow c^a = c^a \bmod n$

8-PGCD – Algorithme Euclide

Soient a, b appartient à Z tels que b≠0 et r le reste de la division euclidienne de a par b. Alors pgcd(a,b) = pgcd(b,r)

Algorithme 1: Euclide (pgcd des deux entiers)

Données : a, b entiers
Résultat : $\text{pgcd}(a, b)$
si $a < 0$ **alors** $a \leftarrow -a$;
si $b < 0$ **alors** $b \leftarrow -b$;
tant que $b > 0$ **faire**
    $\text{temp} \leftarrow b$;
    $b \leftarrow a\%b$;
    $a \leftarrow \text{temp}$;
fin
retourner a ;

La complexité: $O(\log_2 a)$

9-Puissance Algorithme Euclide - Exemple

Soit le calcul de pgcd(25,15).

25 = 15 * 1 + 10 → pgcd(15,10)
15 = 10 *1 + 5 → pgcd (10,5)
10= 5 *2 + 0 → pgcd (5,0)

Donc le pgcd(25,15) = 5.

Puissance Algorithme Euclide – Exemple 2

Soit le calcul de pgcd(1970,1066).

1970 = 1 x 1066 + 904	pgcd(1066, 904)
1066= 1 x 904 + 162	pgcd(904, 162)
904 = 5 x 162 + 94	pgcd(162, 94)
162 = 1 x 94 + 68	pgcd(94, 68)
94 = 1 x 68 + 26	pgcd(68, 26)
68 = 2 x 26 + 16	pgcd(26, 16)
26 = 1 x 16 + 10	pgcd(16, 10)
16 = 1 x 10 + 6	pgcd(10, 6)
10 = 1 x 6 + 4	pgcd(6, 4)
6 = 1 x 4 + 2	pgcd(4, 2)
4 = 2 x 2 + 0	pgcd(2, 0)

Donc le **pgcd(1970, 1066) = 2**

10-Puissance Algorithme d'Euclide étendu

Algorithme de calcul des coefficients u et v tels que : au + bv = d = pgcd(a,b)

Algorithme 2: Euclide étendu (coefficients de Bezout de deux entiers)

Données : a, b entiers

Résultat : (d, u, v) tels que $d = \text{pgcd}(a, b) = au + bv$

si $a < 0$ **alors** $a \leftarrow -a$;

si $b < 0$ **alors** $b \leftarrow -b$;

$u \leftarrow 1, \quad v \leftarrow 0$;

$u_{\text{aux}} = 0, \quad v_{\text{aux}} = 1$;

tant que $b > 0$ **faire**

effectuer la division euclidienne $a = bq + r$;

$a \leftarrow b, \ b \leftarrow r$;

$\text{tmp} \leftarrow u_{\text{aux}}, \ u_{\text{aux}} \leftarrow u - qu_{\text{aux}}, \ u \leftarrow \text{tmp}$;

$\text{tmp} \leftarrow v_{\text{aux}}, \ v_{\text{aux}} \leftarrow v - qv_{\text{aux}}, \ v \leftarrow \text{tmp}$;

fin

retourner (a, u, v) ;

La complexité: $O(\log_2 \max(a,b))$??

Euclide étendu : Exemple

Soit le calcul de pgcd(25,15).

$25 = 15 * 1 + 10 \rightarrow 10 = 25-15$

$15 = 10 *1 + 5 \rightarrow 5 = 15-10 = 15*2-25$

$10= 5 *2 + 0$

Donc le pgcd(25,15)= 15*2 + (-1)*25=5.

Puissance Euclide étendu : Exemple

Soit le calcul de pgcd(120,23).

120 = 23x5 + 5 → 5= 120 – 23x5

23 = 5 x 4 + 3 → 3 = 23 – 5x4 = 23x21 – 120x4

5 = 3x1 + 2 → 2= 5- 3 = 120x5 – 23x26

3 = 2 x1 + 1 → 1 = 3 – 2 = 47x23 – 9x120

Donc le pgcd(120,23)= 120* (-9) + 23*47=1.

11-Inverse modulaire

L'algorithme d'Euclide étendu est une variante de l'algorithme d'Euclide qui permet, à partir de deux entiers a et b, de calculer non seulement leur (PGCD), mais aussi un de leurs couples de coefficients de Bézout (deux entiers u et v tels que au + bv = PGCD(a, b)).

Quand a et b sont premiers entre eux, u est alors l'inverse pour la multiplication de a modulo b (et v est de la même façon l'inverse modulaire de b, modulo a), ce qui est un cas particulièrement utile

•L'inverse modulo n de b est le nombre entier $\mathbf{b^{-1}}$

tel que $\mathbf{b.b^{-1}}$ (mod **n**) = 1 avec b et n sont

premiers entre eux [pgcd(b,n)=1] .

Inverse modulaire: Exemple

•Soit le problème suivant:

trouver $(43)^{-1} \bmod 26$ [=$(17)^{-1} \bmod 26$].

Il vient: 9=26-1*17

8=17-1*9 → 17-1*(26-1*17)=2*17-1*26

1=9-1*8 → (26-1*17-1) * (2*17-1*26)

=2*26 -3*17

On obtient que 2*26-3*17 sous forme au + bv = d avec d=1, u=2 et v= -3.

Donc, (-3) mod 26 = 23 mod 26

l'inverse modulo 26 de 43 est **23**

12-Puissance Equations linéaires modulo n

Considérons l'équation ax = b (mod n), a et b entre 0 et n-1.

- Si a est inversible modulo n [pgcd(a, n) = 1], une solution $x_0 = a^{-1}$ b (mod n). Toute les solutions sont alors de la forme x_0 + kn, avec k dans ZZ.
- Si pgcd(a, n) = d ≠ 1 alors:

  Si d ne divise pas b, alors ax = b mod m n'a pas de solution

  Sinon l'équation précédente est équivalente à àx = b' (mod n') où: à = a/d, b'=b/d et n'=n/d.

Puissance Equations linéaires modulo n : Exemple

Cherchons a résoudre par exemple:

$22x = 55 \bmod 363$

PGCD(22, 363) = 11. comme 11 divise 55, l'équation peut s'écrire: $2x=5 \pmod{33}$

Une solution particuliére est $x_0 = 2^{-1} * 5 = 14*5 = 19 \pmod{33}$.

Toutes les solutions sont données par:

$x = 19+k.33.$

Questions ?