Ministère de l'Enseignement Supérieur et de la Recherche Scientifique Université 08 Mai 1945 - Guelma

Faculté des Sciences Exactes et des Sciences de la Nature et de la Vie Département d'Informatique

3eme année LMD

Sécurité Informatique

Chapitre 2 : Cryptographie

Chargé du cours : Bada Mousâab

Bada.mousaab@gmail.com

Année Universitaire 2015-2016

1. Introduction générale :

La cryptologie est l'étude **des techniques** qui permettent de **protéger l'information** en terme de ***confidentialité***, ***l'authenticité*** et ***l'intégrité***.

Cette discipline comprend :

- **la cryptographie**, qui porte sur la conception de techniques de protection.
- **La cryptanalyse** qui consiste a analyser la sécurité de ces techniques, soit en apportant *une preuve* de sécurité, soit en *démontrant une faiblesse (ex : retrouver le texte claire ou la clef)*.

2. Vocabulaire de base :

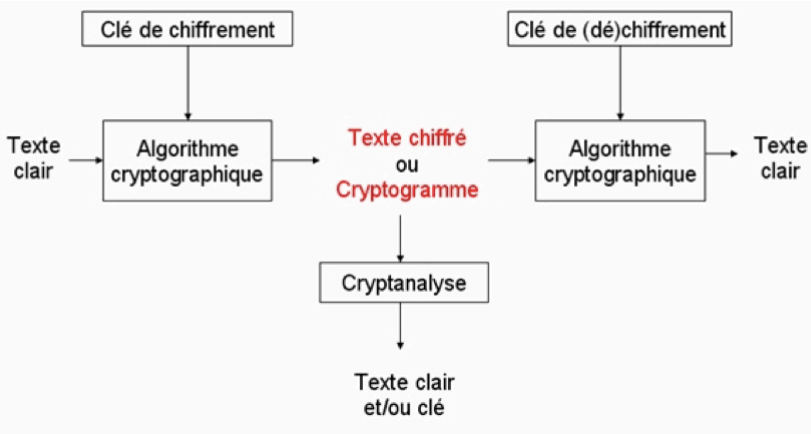


Figure 1 : Protocole de chiffrement

Chiffrement : Le chiffrement consiste à transformer une donnée (texte, message, image, ...) afin de la rendre incompréhensible par une personne autre que celui qui a créé le message et celui qui en est le destinataire.

Déchiffrement : La fonction permettant de retrouver le texte clair à partir du texte chiffré.

Texte chiffré : Appelé également cryptogramme, le texte chiffré est le résultat de l'application d'un chiffrement à un texte clair.

Clef : Il s'agit du paramètre impliqué pour des opérations de chiffrement et/ou déchiffrement.

*Dans le cas d'un **algorithme symétrique**, la clef est **identique** lors des deux opérations.*

*Dans le cas **d'algorithmes asymétriques**, elle **diffère** pour les deux opérations.*

RQ :

- L'algorithme de chiffrement est en réalité un triplet d'algorithmes :
  - Un Algorithme (fonction) générant les clés K.
  - Un Algorithme (fonction) E pour chiffrer le message M.
  - Un Algorithme (fonction) D pour déchiffrer le message C.

- On parle de "**décryptage**" pour désigner l'action permettant de retrouver le texte clair **sans connaître la clef** de déchiffrement.

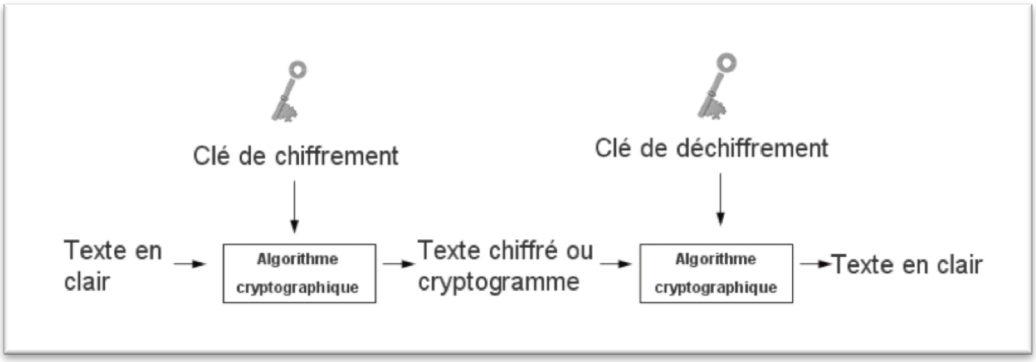
3. Les principaux types d'algorithmes de la cryptographie:

3.1. Crypto-système à base d'une clef symétrique :

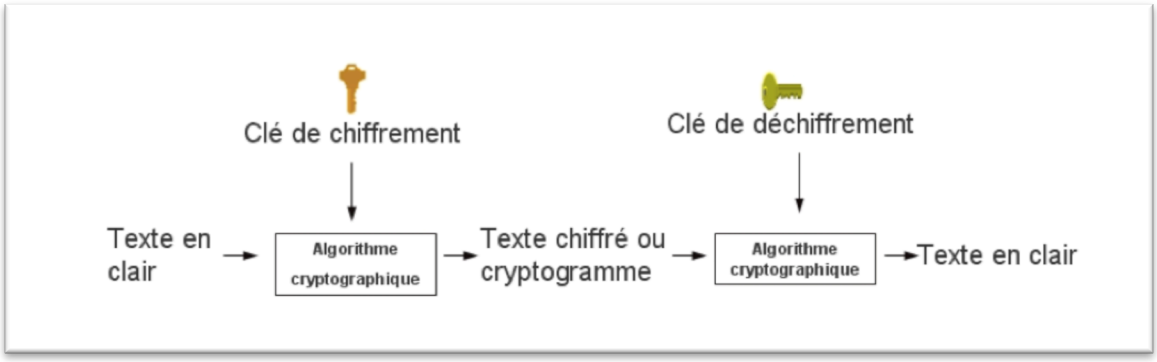
Caractéristiques :

- Les clefs sont identiques : $K_E = K_D = K$.
- La clef doit rester secrète.
- Les algorithmes les plus répandus sont le DES, AES, 3DES, ...
- Au niveau de la génération des clefs, elle est choisie aléatoirement dans l'espace des clefs.
- Ces algorithmes sont basés sur des opérations de transposition et de substitution des bits du texte clair en fonction de la clef.
- La taille des clefs est souvent de l'ordre de 128 bits. Le DES en utilise 56, mais l'AES peut aller jusque 256.

- **L'avantage** principal de ce mode de chiffrement est ***sa rapidité***.
- **L'inconvénient** principal réside dans ***la distribution des clefs***.



3.2. Crypto-système à base d'une clef asymétrique :



Le principe de ce type de chiffrement **ne repose pas** sur l'utilisation d'une clef secrète unique, **mais une paire de clefs** vérifiant une relation mathématique.

Tout le monde, y compris les adversaires peuvent connaître la valeur de la clef publique. Cependant, la clef privée correspondante doit être gardée confidentiellement par son porteur

Caractéristiques :

- Une clef publique P_{Key} (distribuée a tout le monde).
- Une clef privée secrète S_{Key} (une seule entité qui possède cette clef) :
  - Pour Lire le message envoyer par l'émetteur (dans le cas de la confidentialité).
  - Pour Ecrire « chiffrer/envoyer » la signature.
- Propriété : La connaissance de P_{Key} ne permet pas de déduire S_{Key}.
- L'algorithme de cryptographie asymétrique le plus connu est le RSA.
- La taille des clés s'étend de 512 bits à 2048 bits en standard.

- **L'inconvénient principale :** le ***chiffrement asymétrique*** est environ 1000 fois ***plus lent*** que le ***chiffrement symétrique***.

- **L'avantage principale :** ***La distribution des clefs*** est ***très facile***, car l'échange de clefs secrètes n'est plus nécessaire.
  Chaque utilisateur conserve sa clef secrète sans jamais la divulguer ==> Seule la clé publique devra être distribuée.

3.3. Fonction de hachage :

Les fonctions cryptographiques de hachage sont des primitives qui ont pour **objectifs** de **calculer une empreinte cryptographique** à partir de données pouvant être de taille arbitraire. Cette empreinte a une taille fixe selon la fonction de hachage utilisé.
Deux caractéristiques (théoriques) importantes sont les suivantes :

- Ce sont des fonctions unidirectionnelles :
  - A partir de H(M) il est impossible de retrouver M.
- Ce sont des fonctions sans collisions :
  - Il est impossible de trouver $M' \neq M$ tel que $H(M') = H(M)$.

Attention !!! La fonction de hachage ne prend pas une clef cryptographique en paramètre.

3.4. Signature numérique :

La cryptographie à clef publique (asymétrique) rend possible le concept de signature numérique ***si on inverse le processus :***

- Quelqu'un peut signer un message en utilisant sa clef privée, tandis que tout le monde peut vérifier la signature au moyen de clef publique.

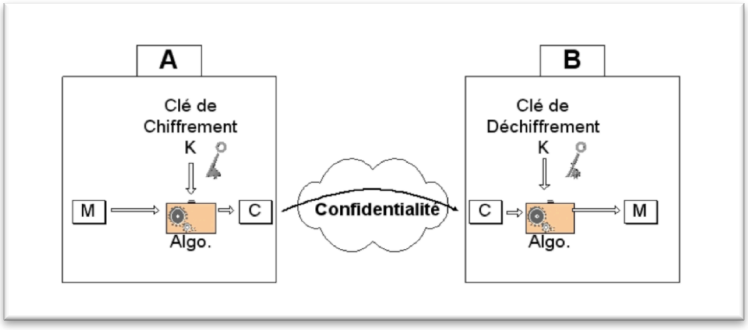
L'objectif de la signature numérique est l'assurance de **non-répudiation**

4. Comment assurer les objectifs principaux de la sécurité ?

4.1. La confidentialité :

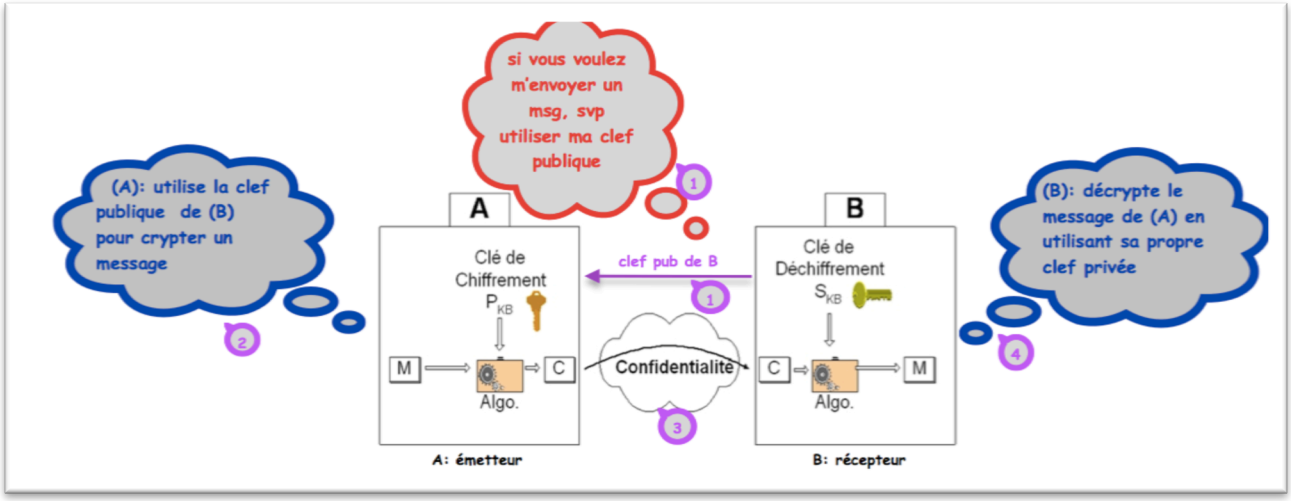
Elle est assurée par le chiffrement du message.

i. Dans le cas de systèmes à clés symétriques, la même clé est utilisée pour $E_{Key}(M)$ et $D_{Key}(C)$. Ce type de chiffrement nécessite un échange préalable de la clé K entre les entités A et B.



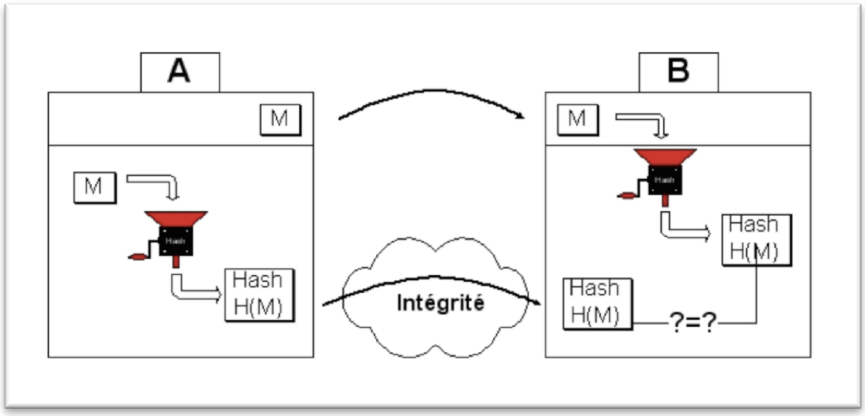
ii. Comme dit précédemment, à l'aide d'un crypto-système asymétrique. Chaque entité possède sa propre paire de clés.

On aura donc la paire (P_{KA}, S_{KA}) pour l'entité A. Et la paire (P_{KB}, S_{KB}) pour l'entité B.



4.2. L'intégrité :

Il faut ici vérifier si le message n'a pas subi de modification durant la communication. C'est ici qu'interviennent les fonctions de hachage.



4.3. L'authenticité

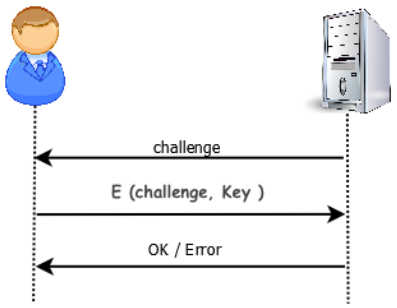
Elle a lieu à plusieurs niveaux.

4.3.1. Au niveau des communiquant :

Un système d'authentification peut utiliser un protocole de type *challenge/réponse,* où le vérificateur (celui qui va vérifier l'identité de l'autre entité) envoie un challenge (défi) au prouveur, qui doit à son tour fournir une réponse correcte pour être authentifié.

Le chalenge est en pratique **une valeur aléatoire** choisie uniformément (avec un probabilité identique) dans un grand ensemble et **utilisée une et une seule fois (**afin d'éviter une attaque dites ***par rejeu*** **)**.

La réponse à ce challenge est généralement produite d'un algorithme de chiffrement symétrique /hachage. Seule la personne qui connaît la clef est en mesure de produire une réponse valide.

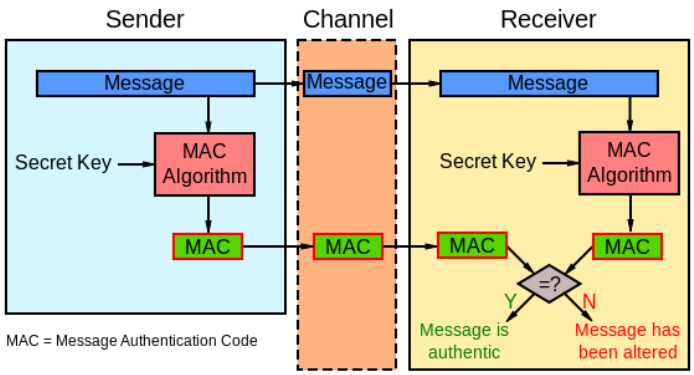


4.3.2. Au niveau de message « code d'authentification de message MAC» :

Les codes d'authentification de message (MAC) sont des primitives cryptographiques construites à partir d'une fonction de hachage, permettant d'assurer l'intégrité et l'authenticité des données.

La grande **différence** est que ce bloc authentificateur ***ne se base plus uniquement*** sur le ***message***, mais également sur ***une clé secrète***.

Objectif : l'intégrité + l'authentification (contre le vol d'une session).



TD2

Exo1 : perte d'une clef privée :

Mohamed qui utilise souvent la messagerie sécurisée de son entreprise, vient de perdre sa clef privée, mais il dispose encore de la clef publique correspondante.

1. peut-il encore envoyer des courriers électroniques chiffrés ? en recevoir ?
2. peut-il encore signer les courriers électroniques qu'il envoie ? vérifier les signatures des courriers électroniques qu'il reçoit ?
3. que doit-il faire pour être de nouveau capable d'effectuer toutes les opérations mentionnées ci-dessus ?

exercice2 : Recherche exhaustive de clefs symétriques :

Sachant que la machine spécialisé « DES-Cracker » met en moyenne 4,5 jours pour retrouver par une recherche exhaustive une clef DES de 56 bits.

1. combien de temps mettrait-elle pour trouver :
   a. une clef DES de 40 bits ?
   b. une clef 3DES de 112 bits ?
   c. une clef AES de 256 bits ?

RQ : on admettra ici que cette machine a besoin du même temps pour chiffrer un bloc de données avec DES, 3DES et AES (ce qui n'est pas le cas en pratique)

Exercice3 :

Un groupe de N personnes souhaite utiliser un système cryptographie pour s'échanger deux a deux des informations confidentielles. Les informations échangées entre deux membres du groupe ne devront pas pouvoir être lues par un autre membre.

Cas1 : le groupe décide d'utiliser un système symétrique de chiffrement.

1. quel est le nombre minimal de clefs symétriques nécessaire ?
2. donner le nom d'un algorithme de chiffrement symétrique reconnu.

Cas2 : le groupe décide ensuite de remplacer ce système par un système asymétrique

1. quel est le nombre minimal de couples de clefs asymétriques nécessaires pour que chaque membre puisse envoyer et recevoir des informations.

Solution exo1 :

Partie1

- Mohamed est encore capable d'envoyer des courriers chiffrés puisqu'il utilise pour cela : la clef publique du destinataire.
- tant qu'il n'aura pas révoqué (annuler) la clef public correspondante à la clef perdue, il recevra encore certainement des courriers chiffrés (personne ne l'empêche), ***MAIS*** il ne sera plus en mesure de les déchiffrer.

Partie2

- il ne peut plus signer les courriers électroniques qu'il envoie puisqu'il utilise pour cela sa propre clef privée.
- il pourra par contre vérifier la signature des courriers qu'il reçoit (utilisant la clef public d'expéditeur)

Partie3

Il est avant tout important de révoquer la clef perdue. Ensuite, il faut se procurer un nouveau couple de clefs publique et privée.

Exo2 :

Sachant que « DES-Cracker » met en moyenne 4,5 jours (soit 388 800 secondes) pour retrouver une clef DES de 56 bits,

Le cassage d'une clef de 40 bits nécessite en moyenne

- $(2^{40}/2^{56})*388\ 880= 5{,}9$ seconde

Alors qu'une clef de 112 bits

- $(2^{112}/2^{56})*4{,}5 = 3{,}24 * 10^{17}$ jours = $9* 10^{14}$ année = 13 milliard annee * 68290
- $(2^{112}/2^{56})*388\ 880= 2{,}8 * 10^{22}$ s

et une clef de 256 bits :

$(2^{256}/2^{56})*388\ 880= 6{,}3 * 10^{65}$ s

Ces deux derniers nombres représente des durée respectives de 68290 fois $1{,}5* 10^{48}$ fois l'âge de l'univers (13 milliard d'années)

RQ : il est intéressant qu'il faut en moyenne 4,5 jours de calcul pour retrouver une clef de DES 56 bits avec DES cracker, ce qui signifie qu'il faut dans le pire des cas 9 jours de calcul à cette **machine pour retrouver La clef DES de 56 bits** ➔ c'est a dire pour tester les 2^{56} clef possible.

Exo3 :

1. Les informations échangées entre deux membres du groupe ne devant pas être lu par un autre membre

➔ Il est nécessaire d'avoir une clef symétrique par couple de correspondant potentiels.

- La 1ere personne a besoin de (N-1) clefs pour communiquer avec les (N-1) personnes qui reste ➔ pourquoi le « -1 » ? ➔ il n'aura pas besoin d'une clef pour communiquer avec lui-même o_O'' c'est pour ca on a fait N-1.

  Key1_2 pour communiquer avec la 2eme personne.
  Key1_3 pour communiquer avec la 3eme personne.
  Key1_4 pour communiquer avec la 4eme personne.
  ...
  Key1_N pour communiquer avec la Neme personne.
  De 2 jusqu'à N : on a N-1 clef

- Pour que la 2eme personne puisse communiquer avec les autres, on a besoin de ***(N-2) nouvelles clefs.*** ➔ Pourquoi pas N-1 comme la 1ere personne??? ➔ la 2eme personne n'a pas besoin d'une nouvelle clef pour communiquer avec la 1ere personne (elle utilise key1_2, parce que l'algorithme de chiffrement est symétrique)

  Liste des nouvelles clefs :
  Key2_3 pour communiquer avec la 3eme personne
  Key2_4 pour communiquer avec la 4eme personne
  Key2_5 pour communiquer avec la 5eme personne
  ...
  Key2_N pour communiquer avec la Neme personne
  De 3 jusqu'à N : on a N-2 clef

- Etc..

Soit en total : (N-1) + (N-2) + ...+3+2+1 = N*(N-1)/2 clefs

2. voici quelques exemple d'algorithme symétriques reconnus : AES, 3DES, Camellia ...

3. Chaque membre du groupe doit posséder un couple (clef publique, clef privée) ➔ il faudra donc au minimum N couple de clefs dans le groupe