

# Sécurité Informatique

## CHAPITRE 1: Introduction à la sécurité informatique

### 1- Définition:

La sécurité informatique vise à protéger les systèmes contre les menaces accidentelles ou intentionnelles en utilisant diverses mesures de protection.

### 2- Principaux concepts de sécurité informatique:

- Menace : risque potentiel qui peut compromettre la sécurité d'un système informatique, telles que les attaques de hackers, les virus, et les accès non autorisés.
- Vulnérabilité : point faible ou une faille dans un système ou une application qui peut être exploitée par une menace pour compromettre la sécurité, comme des logiciels obsolètes ou des configurations incorrectes.
- Contre-mesure : stratégies, outils ou pratiques mises en place pour atténuer les risques de sécurité en identifiant, prévenant ou réduisant les menaces et les vulnérabilités, tels que les mises à jour de sécurité, les pare-feu, le chiffrement des données, des Antivirus, formation à l'usage.

### 3- Principaux objectifs de la sécurité informatique:

Continuité de service : un service doit être assuré avec un minimum d'interruption.

- Disponibilité : Assurer que les systèmes et les données sont accessibles et utilisables lorsque nécessaire, et qu'ils ne sont pas indisponibles en raison d'incidents de sécurité. (garantir l'accès aux ressources nécessaires)
- Intégrité : Garantir que les données ne sont ni modifiées ni altérées de manière non autorisée ou non intentionnelle.

- Confidentialité : Assurer que seules les personnes autorisées ont accès aux données sensibles et qu'elles ne sont pas divulguées à des tiers non autorisés pour assurer la confidentialité des données, il faut limiter et contrôler l'accès aux personnes autorisées et chiffrer les données.
- Authentification : consiste à vérifier l'identité d'une entité avant de lui accorder l'accès à une ressource, généralement à l'aide de mots de passe ou d'empreintes biométriques.
- Non réputation : empêcher les utilisateurs de nier leurs actions ou transactions effectuées sur un système.

#### 4- Définitions : crime informatique et cybercrime :

- Le cyberspace : un milieu numérique mondial de communication et d'information.
- Un crime informatique : le crime informatique implique l'utilisation d'un système informatique comme objet ou moyen pour commettre un délit, étant ainsi lié aux technologies numériques.
- Le cybercrime : est une facette du crime informatique utilisant les technologies internet pour commettre des délits, englobant toutes les infractions réalisées dans le cyberspace.

#### 5- Les Attaques informatiques :

Les attaques informatiques exploitent les failles des systèmes informatiques, avec des intrus cherchant à satisfaire leur curiosité, à obtenir un avantage financier ou commercial, à démontrer leur intelligence, à causer des dégâts ou à analyser les vulnérabilités pour les corriger.

## \* Origine des attaques:

- interne : sont le fait d'individus ou d'entités ayant un accès légitime au système, comme des employés malveillants ou sous-traitants, qui abusent de leurs priviléges d'accès.
- externe : sont initiées par des entités extérieures au réseau ou au système cible, telles que des hackers, des organisations criminelles, des groupes d'activistes ou même des états-mitiges.

## \* Taxonomie des attaques:

- La Taxonomie des attaques informatiques distingue 2 types d'attaques :
- **Attaque passive** : implique l'écoute et l'interception des communications entre les parties sans alterer les données en transit, visant principalement à collecter des informations sensibles ou à surveiller le trafic réseau.
  - **Attaque active** : implique une action directe de la part de l'attaquant pour alterer, manipuler ou perturber les données ou les systèmes cibles, souvent dans le but de compromettre la sécurité, de causer des dommages ou de tirer un avantage illégitime.

## \* Attaques Virales: Les virus malveillants:

- **Virus informatique** : programme malveillant capable de modifier d'autres programmes pour se reproduire.
- **Cheval de Troie (Trojan)** : programme malveillant dissimulé dans un autre, permettant un accès à distance à la machine victime.
- **Bombe logiques** : programme malveillant dupliqué sur plusieurs machines, activé à un moment précis pour attaquer une cible spécifique.

- Logiciel espion (spyware): Logiciel malveillant qui collecte des informations sur la machine infectée.

### \* Atttaques de reconnaissance:

Consistent à balayer le réseau pour identifier les @ IP actives, les ports ouverts, les systèmes d'exploitation et les versions de logiciels, souvent utilisant des outils tels que les Sniffers de paquets comme Wireshark, afin d'espionner les communications réseau, les e-mails, les identifiants de connexion et l'activité web des utilisateurs.

### \* Atttaques par devinette:

Vise à trouver un MDP en utilisant soit une méthode de force brute, qui teste toutes les combinaisons possibles, soit une attaque par dictionnaire qui teste des mots prélevés dans un dictionnaire de mots couramment utilisés

comme MDP potentiels.

### \* Atttaques de Dénie de Service (DDoS):

Une Atttaque de déni de service (DOS & DDoS) perturbe ou ralentit un service, générant un volume élevé de trafic ou un trafic mal formé, tandis qu'une attaque distribuée (DDoS) implique plusieurs sources coordonnées pour produire V

### \* Atttaques MAN-IN-THE-MIDDLE:

Implique qu'un intermédiaire intercepte et modifie les communications entre 2 parties en se positionnant au milieu, souvent en fournitant des services de point d'accès ou de passerelle réel sans que la victime ne soit consciente de la manipulation.

Publi: En charge, le serveur  
Aspirer  
HOAX: Sensibiliser les utilisateurs afin de partager un message.

{ + Spamming: l'envoi massif et non sollicité de courriels ou de messages indésirables à des destinataires sans leur consentement.

### 6- Mécanismes de Sécurité:

- Notarisation, tamponnage (Timestamping), Détection d'intrusion, Pare-feu (filtrage), Antivirus, stéganographie, chiffrement, Signature Numérique.

(4)

## CHAPITRE 2 : Cryptographie classique.

### 1- introduction:

La sécurité informatique utilise la cryptographie, divisée en 2 grandes familles cryptographie classique et moderne pour protéger les systèmes contre les attaques.

### 2- Concepts de base :

- \* La cryptologie : elle étudie scientifiquement les techniques de cryptographie et de la cryptanalyse
- \* La cryptographie : elle englobe les méthodes pour rendre les messages incompréhensibles.
- \* La cryptanalyse : elle vise à casser les fonctions cryptographiques existantes pour évaluer leur sécurité.
- \* La stéganographie : elle dissimule un secret dans un support apparemment anodin (inoffensif), comme des images ou un texte.
- \* La stéganographie classique : elle consiste à cacher un message secret à l'intérieur d'un autre message. exemple: collecter des images en poussière

### 3- Cryptographie:

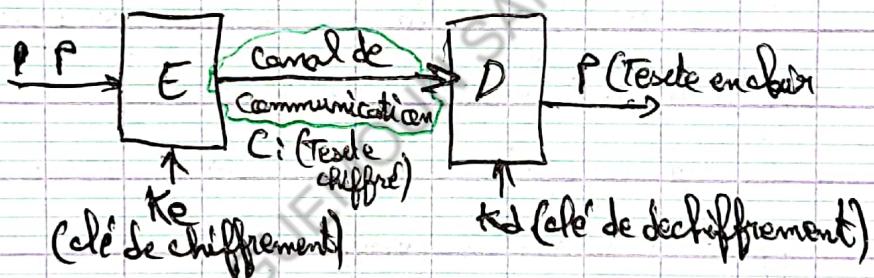
#### 1- Définition: crypte → cache' graphy → écriture

La cryptographie est une discipline ancienne qui vise à protéger les messages en les transformant via le chiffrement, rendant le texte en clair ( $P$ ) incompréhensible pour former le texte chiffré ( $C$ )

## 2- Terminologie :

- \* Algorithme de chiffrement (E): Transforme un texte en clair en un message chiffré.
- \* Clé de chiffrement ( $k_e$ ): informations secrètes utilisées avec l'algorithme de chiffrement pour crypter le texte en clair.
- \* Algorithme de déchiffrement (D): reconstitue le texte en clair à partir du message chiffré.
- \* Clé de déchiffrement ( $k_d$ ): informations secrètes utilisées avec l'algorithme de déchiffrement pour décrypter le texte chiffré et le convertir en texte clair.

## 3- Principe :



## 4- Cryptanalyse :

- \* Attaque à texte chiffré seulement: la cryptanalyse cherche à déterminer des textes en clair où à retrouver la clé en ayant uniquement accès aux textes chiffrés.
- \* Attaque à texte en clair connu: la cryptanalyse utilise des textes en clair et leurs équivalents chiffrés avec la même clé pour déterminer cette clé.
- \* Attaque à texte en clair choisi: la cryptanalyse, en plus des textes en clair et chiffrés, peut choisir un texte spécifique et observer sa transformation pour déterminer la clé.

## 5. Algorithmes classiques:

- \* chiffrement par substitution: remplace chaque symbole ou ensemble de symboles du texte en clair par un autre symbole ou ensemble de symboles pour obtenir le texte chiffré.
- \* chiffrement par transposition (permutation): les positions des symboles du texte en clair sont échangées ou permutees avec les positions d'autres symboles pour obtenir le texte chiffré.

## 6. Chiffrement par substitution:

- \* La substitution monoalphabétique: remplace chaque symbole du texte en clair par un autre symbole unique pour obtenir le texte chiffré; exemples incluent le code de César, le chiffrement affine et le chiffrement monoalphabétique aléatoire.

- \* La substitution polyalphabétique: utilise une suite périodique de substitutions monoalphabétiques où un même symbole peut être remplacé par plusieurs symboles; exemple: chiffrement de Vigenère

- \* La substitution de polygramme: substitue un groupe de  $m$  symboles dans le texte en clair par un autre groupe de  $m$  symboles; exemples incluent le chiffrement à Hill et le chiffrement de Playfair (ms 2)

## 7. Code de César:

- consiste à décaler les lettres de l'alphabet d'un nombre  $K$

qui représente la clé.

exemple:  $K=3$

Texte en clair: sécurité

Texte chiffré:

VHFXULWHD

chiffrement:

$$(18+3) \bmod 26 = 21$$

$\xrightarrow{S}$  clé

$$21 - 27 \bmod 91 = 10$$

Chiffrement:  $C = E_K(P) = (P + K) \bmod 26$

Déchiffrement:  $P = D_K(C) = (C - K) \bmod 26$

$K$ : clé de chiffrement.  $E$ : fonction de chiffrement.  $D$ : fonction de déchiffrement

$P$ : lettre en clair  $C$ : lettre chiffrée

- cryptanalyse par force brute ou attaque exhausive  
- cryptanalyse par analyse de fréquence

③

## 8 - Cryptanalyse par analyse de fréquences des lettres:

- Texte chiffré contenant 100 lettres avec la lettre "T" apparaissant 25 fois. (Texte chiffré page 14 du cours)
- la fréquence d'apparition de "T" est de 25% suggérant que "E" est chiffré par "T" donc  $k=15$

## 9 - Chiffrement AFFINE:

faut d'abord vérifier que:

$$(a, b) \in \mathbb{Z}_{26} \times \mathbb{Z}_{26}$$

et  $\text{PGCD}(a, 26) = 1$

- fonction de chiffrement dans  $\mathbb{Z}_{26}$ :  $C = (ap + b) \bmod 26$  où  $p$  est la lettre en clair,  $C$  est la lettre chiffrée, et  $a$  et  $b$  sont les paramètres de la clé de chiffrement.
- si  $a = 1$ , le chiffrement affine se réduit au chiffrement de César où  $b$  représente le décalage.
- si  $a$  et  $26$  sont premiers entre eux, alors  $a^{-1}$  a un inverse à  $\bmod 26$
- fonction de déchiffrement dans  $\mathbb{Z}_{26}$ :  $p = a^{-1}(C - b) \bmod 26$

## 10 - Chiffrement monocryptographique:

- permet une substitution aléatoire de chaque lettre par une autre
- dans un alphabet de 26 caractères, la clé est formée de 26 caractères distincts représentant les substitutions de chaque lettre.
- exemple: Si A est substitué par P, B par S, C par Y... la clé serait (P S Y ... T)
- Le nombre de possibles clés possibles est  $26!$ , ce qui signifie  $26 \times 25 \times 24 \times \dots \times 2 \times 1$  soit un très grand nombre de possibilités.

## 11. Chiffrement de VIGENÈRE :

Câine de Vigenère :

Page 19 du

Cours

- est un chiffrement de substitution polyalphabétique.
- il améliore le chiffrement de César en utilisant un mot-clé où chaque lettre indique le décalage alphabétique à appliquer sur chaque lettre du texte en clair.
- exemple : avec le mot-clé "BONJOURB" et le texte en clair "SECURITE".  
Chaque lettre de "BONJOURB" correspond à un décalage alphabétique à appliquer sur chaque lettre de "SECURITE".

clé : BONJOURB  
 1 14 13 9 14 20 14 1 }  
 Texte en clair : SECURITE  
 18 4 2 20 14 8 19 }  
 19 18 15 3 5 2 10 5 }  
 T S P D F E K F  
 pour son déchiffrement

$$P = (C - k) \bmod 26$$

Remarque :  $x \bmod y$

si  $x > 0$ :

$x \bmod y = \text{reste div de } x \text{ par } y$

si  $x < 0$ :

$x \bmod y ; x + y + y \text{ jusqu'à } x > 0 \text{ et } x < y$

## 12. Chiffrement de PLAYFAIR :

Le chiffrement de PLAYFAIR utilise une grille  $5 \times 5$  contenant 25 lettres de l'alphabet (Toutes sauf le W, qui est remplacé par V)

Dans la variante Anglaise, on conserve le "W" et les lettres "I" et "J" sont fusionnées.

Pour former la grille de chiffrement, on utilise un mot-clé secret pour créer un alphabet discordant. Les lettres de ce mot-clé sont placées dans la grille ligne par ligne. Ensuite, les autres lettres de l'alphabet sont ajoutées dans l'ordre pour compléter la grille.

Exemple : Mot-clé = SALUT

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

on chiffre le texte par groupe de 2 lettres en appliquant les 4 règles qui suivent :

- ① Si les 2 lettres en clair forment le coin d'un rectangle dans la grille  $5 \times 5$ , les lettres chiffrées sont les coins opposés. La première lettre chiffrée est sur la même ligne que la première lettre en clair, exemple : AF chiffre en TC.
- ② Si 2 lettres sont sur la même ligne dans la grille, on prend les 2 lettres qui les suivent immédiatement à leur droite, exemple : SL est chiffré en AV.
- ③ Si les 2 lettres sont sur la même colonne dans la grille, on prend les 2 lettres qui les suivent immédiatement en dessous : TR est chiffré en EZ.
- ④ Si un groupe de lettres à chiffrer est composé de la même lettre, on ajoute "X" entre les 2 lettres. LL devient LX.

### 13- Le chiffrement de Hill:

- ① chaque lettre est remplacée par son ordre dans l'alphabet : A devient 0, B devient 1, ..., Z devient 25.
- ② les nombres ainsi obtenus sont regroupés en blocs de taille m.
- ③ pour chaque bloc m- nombres à coder, on calcule le texte codé en effectuant des combinaisons linéaires avec une clé k sous forme d'une Matrice carrée d'ordre m.
- ④ le déchiffrement peut être effectué en utilisant la Matrice inversée.

⑤

⑤ La Matrice K est inversible si  $\det(K) \neq 0$  (car  $\det(K)^{-1} = 1/\det(K)$ ) où  $\det(K)$  est le déterminant de la Matrice K.

#### 14 - Transposition simple par colonnes :

##### Chiffrement :

- ① Disposer les lettres du message clair horizontalement sur une Matrice.
- ② Le nbr de colonnes dans la Matrice est déterminé par un paramètre n.
- ③ Collecter verticalement les lettres de la Matrice pour former le texte chiffre.

##### Déchiffrement :

- ① Disposer verticalement les lettres du Message chiffre'.
  - ② Collecter horizontalement les lettres pour recomposer le texte en clair.
- Exemple : Texte en clair : "CHIFFREMENT DE CESAR"; nbr colonnes n=5  
Texte chiffre' : "CRTSHEDAIMERFECFINE"

#### 15 - Transposition complexe par colonnes :

##### Chiffrement :

- ① Définir une clé de chiffrement.
- ② Disposer horizontalement les lettres du Message clair sur une Matrice avec un nombre de colonnes équivalents à la longueur de la clé.
- ③ Collecter verticalement les lettres selon l'ordre défini par la clé.

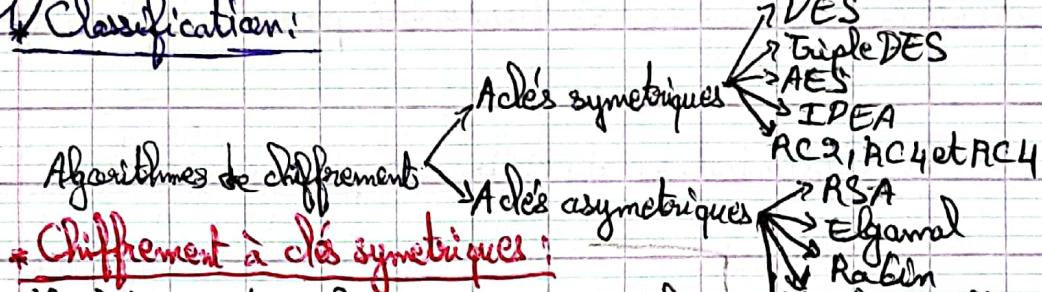
##### Déchiffrement :

- ① Disposer verticalement les lettres du Message chiffre suivant la clé.
  - ② Collecter horizontalement les lettres pour retrouver le Texte en clair.
- Exemple : Texte en clair : "CHIFFREMENT DE CESAR"  
clé de chiffrement : "15423"  
Texte chiffre' : "CRTSFECFINEIMERHOPA"

## CHAPITRE 3: Cryptographie Moderne

### A- Algorithmes de chiffrement modernes:

#### 1/ Classification:



#### 2 Chiffrement à clés symétriques :

Le chiffrement à clé symétrique utilise une seule clé pour chiffrer et déchiffrer des données, offrant rapidité et efficacité, mais nécessitant une distribution sécurisée des clés. (l'émetteur et le récepteur doivent posséder la même clé secrète)



#### 3 Chiffrement à clés asymétriques (à clé publique) :

Le chiffrement à clés asymétriques, également appelé chiffrement à clé publique, est une méthode de cryptage où une paire de clés distinctes, une clé publique et une clé privée, est utilisée pour chiffrer et déchiffrer des données, offrant ainsi des avantages tels que la sécurité des communications et la vérification d'identité. En utilisant la clé publique du destinataire pour chiffrer et sa propre clé privée pour déchiffrer, le chiffrement asymétrique garantit la confidentialité des messages.

#### 2- Avantages et inconvénients : - : inconvénient - : avantages .

#### Le chiffrement à clés symétriques offre une rapidité et une efficacité

grâce à l'utilisation de clés de taille relativement faible, mais souffre de problèmes de distributions et de gestion des clés secrètes. En revanche, le chiffrement à clés

de distribution de clés.

asymétriques résout ces problèmes en utilisant des paires de clés distinctes, mais au prix d'une lenteur et d'une charge de calcul accrue dues à l'utilisation de clés plus longues et à des exigences de traitement processeur plus importantes.

### 3 - Optimisation du chiffrement par une clé de session :

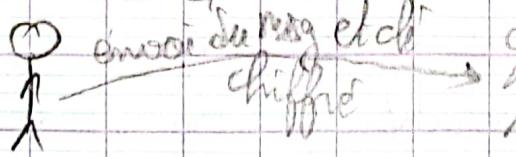
Comment combiner l'usage des 2 systèmes de chiffrement ?

App → Pour combiner l'usage des deux systèmes de chiffrement, on utilise un algorithme symétrique et une clé de session pour chiffrer les messages de grande taille, tandis qu'un algorithme asymétrique est utilisé pour différer la clé de session. Une clé de session est une clé secrète partagée entre 2 interlocuteurs pendant la durée de l'échange et détruite à la fin de la session de travail.

Pour assurer la confidentialité des données échangées entre 2 entités, l'émetteur génère aléatoirement une clé de session, chiffre le message avec cette clé utilisant un algorithme symétrique, puis chiffre la clé de session avec la clé publique du destinataire via un algorithme asymétrique. Le message chiffré et la clé de session chiffrée sont envoyés au destinataire. Ce dernier déchiffre la clé de session avec sa clé privée, puis déchiffre le message avec cette clé de session. Enfin, le destinataire peut utiliser cette clé de session pour échanger des messages chiffrés avec son interlocuteur.

① l'un des deux algorithmes de chiffrement

- ② chiffrer msg. avec clé session et algo sym.
- ③ chiffrer la clé session avec la clé pub du destinataire (algo asymétrique)



④

- ⑤ déchiffrez la clé de session avec sa clé privée
- ⑥ déchiffrez le msg avec la clé de session

- Tenir sa sécurité du logarithme discret  $\Rightarrow A = B^x \bmod p$
- Le protocole est vulnérable à l'attaque Man in the Middle (MitM)

Objectif: partage au échange de données d'une clé secrète par intermédiaire d'un échange de données publiques.

## II/ Protocole de DIFFIE-HELLMAN (DH): (asymétrique)

permet à 2 participants A et B d'établir un secret partagé sur un canal de communication non sécurisé. Voici comment cela fonctionne :

- ① Choix des paramètres : les 2 participants choisissent publiquement un nombre premier  $p$  et une base  $g$  (un entier plus petit que  $p$ ), qui servent de paramètres de DIFFIE-HELLMAN
- ② Génération des clés privées : chaque participant génère confidentiellement sa propre clé privée :

- A génère  $x_A$  tel que :  $x_A < p$
- B génère  $x_B$  tel que :  $x_B < p$

- ③ Calcul des clés publiques : chaque participant calcule alors sa clé publique

- A calcule :  $y_A = g^{x_A} \bmod p$
- B calcule :  $y_B = g^{x_B} \bmod p$

- ④ Echange des clés publiques : les 2 participants s'échangent leurs clés publiques  $y_A$  et  $y_B$

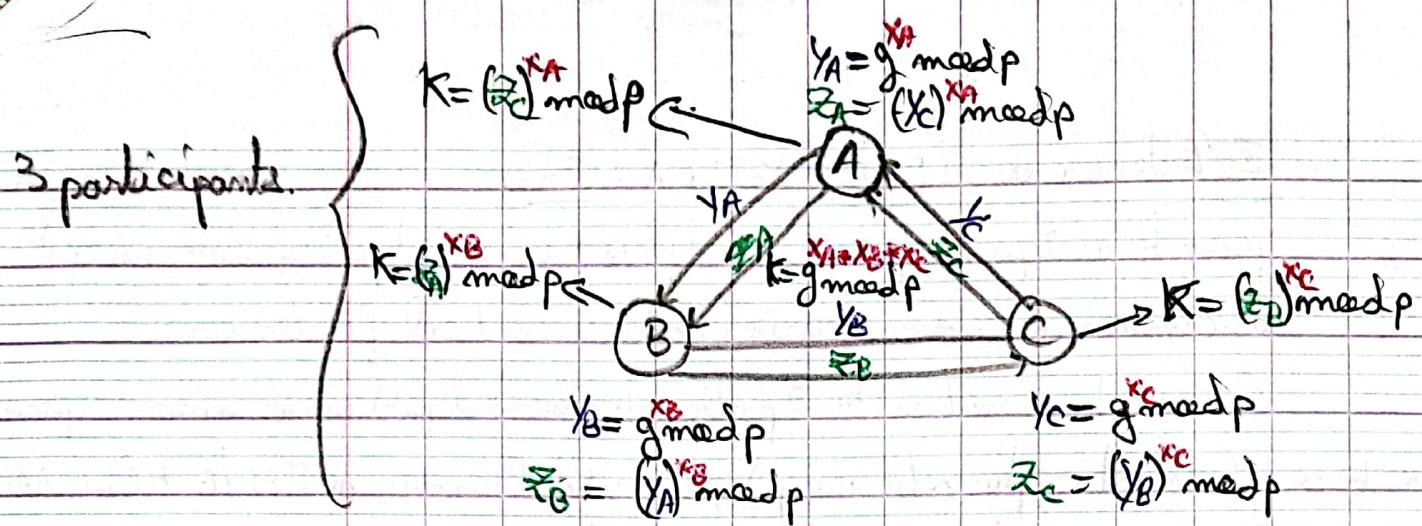
- ⑤ Calcul de la clé secrète : chaque participant calcule la clé secrète en utilisant la clé publique de l'autre participant et sa propre clé privée :

- A calcule :  $K = (y_B)^{x_A} \bmod p$
  - B calcule :  $K = (y_A)^{x_B} \bmod p$
- } Clé K constitue le secret partagé entre les 2 participants.

$$\begin{array}{ccc}
 y_A = g^{x_A} \bmod p & & y_B = g^{x_B} \bmod p \\
 \textcircled{A} & \xrightarrow{\hspace{1cm}} & \textcircled{B} \\
 \downarrow & & \downarrow \\
 K = (y_B)^{x_A} \bmod p = g^{x_A \cdot x_B} \bmod p & = & K = (y_A)^{x_B} \bmod p
 \end{array}$$

- A et B partagent 2 paramètres ( $p, g$ ). - clé privée de A  $\Rightarrow x_A$
- clé privée de B  $\Rightarrow x_B$ . - clé publique de A  $\Rightarrow y_A$ .
- clé publique de B  $\Rightarrow y_B$

③



### III/ Chiffrement de RSA :

RSA est un algorithme de cryptographie à clé publique inventé par Ron Rivest, Adi Shamir et Leonard Adleman en 1977, qui repose sur le problème de factorisation pour assurer sa sécurité. (asymétrique)

#### Génération des clés :

- 2 grands nombres premiers  $p$  et  $q$  (distincts) sont choisis ( $p \neq q$ )
- calculer  $n = p * q$
- calculer  $\phi(n) = (p-1) * (q-1)$
- un entier  $e$  est choisi tel que :  $1 < e < \phi(n)$  et que  $\text{pgcd}(e, \phi(n)) = 1$
- calculer  $d$  tel que :  $e * d \mod \phi(n) = 1$  avec  $1 < d < \phi(n)$
- la clé publique  $(e, n)$ , la clé privée  $(d, n)$

#### Chiffrement : pour chiffrer un texte $M$ :

$$C = M^e \mod n \quad \text{et tel que: } M < n \quad (\text{M: texte clair, C: texte chiffré})$$

#### Déchiffrement : pour déchiffrer un texte chiffré $C$ :

$$M = C^d \mod n.$$

Exercice (page 13 du cours).

## IV/ Chiffrement d'Elgamal:

Chiffrement d'Elgamal est un système de cryptographie asymétrique qui repose sur la difficulté du problème du logarithme discret. Il permet à un expéditeur de chiffrer un message en utilisant la clé publique du destinataire, qui peut ensuite le déchiffrer en utilisant sa propre clé privée.

### Génération des clés:

- Choisir un grand nombre premier p et 2 nombres a et g tel que:

$$a < p \text{ et } g < p$$

- Calculer  $A = g^a \bmod p$

- Clé publique  $(A, g, p)$  Clé privée  $(a)$

### Chiffrement: $M < p$

- Choisir un nombre aléatoire b ( $b < p$  et  $\text{pgcd}(b, p-1) = 1$ )

- calculer  $B = g^b \bmod p$

- Calculer  $C = (M \times A^b) \bmod p$

- le chiffre du Message  $(B, C)$

### Déchiffrement:

$$M = (C \times B^{(p-a-1)}) \bmod p$$

## V/ Fonction de Hashage:

-  $h = H(M)$ : h est appelé le hash, le condensé ou l'empreinte tel que: h est de longueur fixe et inférieure à M.

- propriétés d'une fonction de hashage.

- exemples : MD4, MD5, SHA-1

- MAC : Message Authentication Code

⑤

## ✓ Signature Numérique :

### \* Signature Numérique avec RSA :

- Paire de clés de l'expéditeur  $\Rightarrow \{(\text{e}, \text{m}), (\text{d}, \text{m})\}$
- Expéditeur  $\Rightarrow$  Génération de la signature de M
  - calcule une empreinte de message (hash) :  $h = H(M)$
  - calcule la signature :  $S = h^d \bmod m$ , où d est la clé privée et m est le module RSA
  - La Signature numérique est :  $(M, S)$
- Destinataire  $\Rightarrow$  vérification de la signature
  - calcule une empreinte de message  $h_1 = H(M)$
  - calcule  $h_2 = S^e \bmod m$ , où e est la clé publique et m est le Module RSA.
  - si  $h_1 = h_2$ , la signature est valide.

En résumé, l'expéditeur génère une signature numérique en prenant l'empreinte du message, puis en la chiffrant avec sa clé privée. Le destinataire vérifie cette signature en déchiffrant la signature avec la clé publique de l'expéditeur et en comparant le résultat avec l'empreinte du message. Si les empreintes concordent, la signature est valide.

### \* Signature Numérique avec ElGamal :

- Paire de clés de l'expéditeur  $\Rightarrow \{(\text{A}, \text{g}, \text{p}), \text{a}\}$
- Expéditeur  $\Rightarrow$  Génération de la Signature de M
  - calcule une empreinte de message :  $h = H(M)$
  - choisit un nombre aléatoire b tel que  $b < p$  et  $\text{pgcd}(b, p-1) = 1$  où p est un nombre premier et g est un générateur du groupe multiplicatif ( $\bmod p$ )

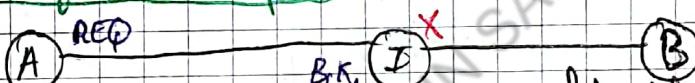
- Calcule  $B = g^b \text{ mod } p$
- Calcule  $C = \text{tel que } h = (axB + bxC) \text{ mod } (p-1)$
- La Signature est:  $(M, S)$  où  $S = (B, C)$

\* Destinataire  $\Rightarrow$  vérification de la signature:

- Calcule une empreinte de message:  $h' = H(M)$
- Si  $(A^B \times B^C) \text{ mod } p = g^h \text{ mod } p$ , alors la signature est valide.

En résumé, l'expéditeur génère une signature numérique en utilisant ED25519 en choisissant aléatoirement un nombre  $b$ , calculant  $B$  et  $C$  à partir de ce nombre, puis en les incluant dans la signature. Le destinataire vérifie ensuite la signature en utilisant les valeurs de la signature et en vérifiant si une équation spécifique est satisfaite. Si elle est satisfaite, la signature est valide.

## VII/ Les Certificats numériques:



- A envoie à B une requête pour avoir sa clé publique.
- I intercepte la requête.
- I répond à A avec  $(B, K_A)$  en se faisant passer pour B.

Un certificat d'identité: est un document électronique signé par une autorité de certification (AC) qui lie une entité à sa clé publique, assurant ainsi la validité de la liaison entre les deux.

### Structure d'un certificat standard X.509:

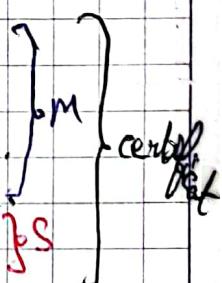
- Version du Standard. - Numéro de Série du certificat.

- Fonction de hashage utilisée. - Algô de signature utilisée.

- L'identité du Signataire - Période de validité du certificat.

- L'identité de l'utilisateur. - la clé publique de l'utilisateur.

- Signature de l'autorité de confiance.



### Certificat d'attribut:

Un certificat d'attribut contient un ensemble d'attributs qui

définissent les permissions ou les droits accordés à son titulaire.

## V.7.7 / Modèles de certification:

- Dans un modèle hiérarchique, une autorité racine délivre des certificats d'attributs, permettant la délégation de l'autorité à d'autres entités, tandis que dans un Modèle croisé, les autorités racines de différentes organisations signent mutuellement des certificats, facilitant la vérification des clés publiques entre les utilisateurs.
- Dans un modèle de certification en graphe, chaque autorité de certification émet un certificat d'identité à une autre autorité en laquelle elle a confiance. Dans un modèle de certification complètement distribué, chaque utilisateur peut éigner et émettre des certificats pour d'autres utilisateurs, formant ainsi un réseau de confiance, tel que PGP (Pretty Good Privacy), où si A fait confiance à B et B fait confiance à C, alors A peut faire confiance à C.

les dessins page 23, 24, 25, 26 dans le cours.

les exemples page 27, 28, 29, 30, dans le cours.

## \* Autorités de certification et PKI:

- La PKI (infrastructure à clé publique) gère et sécurise les échanges d'informations en utilisant des algorithmes, protocoles et services, comprenant une procédure de certification en 3 étapes: enregistrement de l'utilisateur, génération de la paire de clés et certification par l'autorité de certification avec publication du certificat sur un annuaire.
- La PKI fournit les services de génération et de mise à jour de paires de clés, de certification des clés publiques avec publication des certificats ainsi que de revocation des certificats, incluant l'extraction, la divulguation de la clé privée et la perte de confiance de l'utilisateur.