

Cours	Introduction à la Sécurité Informatique
Auditoire	LA3RT & LA3GL (INSAT) L_BD_3 & MP_Cyber (UC)
Établissement	INSAT/UC
Responsable du cours	Marwa CHAIEB
Années Universitaires	2018/2019 (INSAT) 2020/2021 (UC)

Description du cours

Ce cours permet la compréhension de la sécurité informatique à travers la présentation des concepts de base utilisés. Il analyse les principaux objectifs et propriétés de la sécurité informatique (confidentialité, intégrité, authentification, authenticité ...)

Chaque séance traite un point important illustré par des exemples, exercices et travaux pratiques.

A la fin du cours, l'étudiant sera capable de comprendre les spécificités des différents éléments.

Objectifs du cours :

À l'issue de ce cours, l'étudiant(e) doit être capable de :

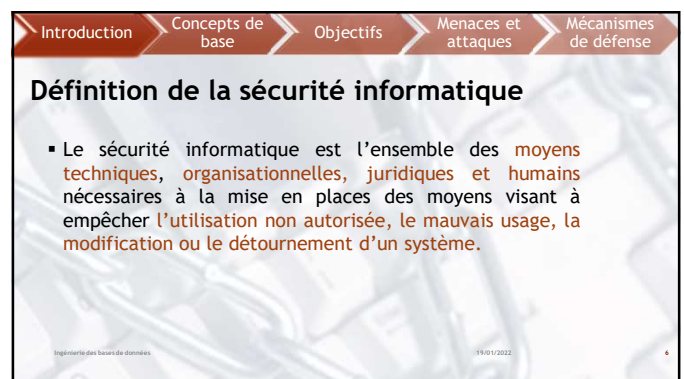
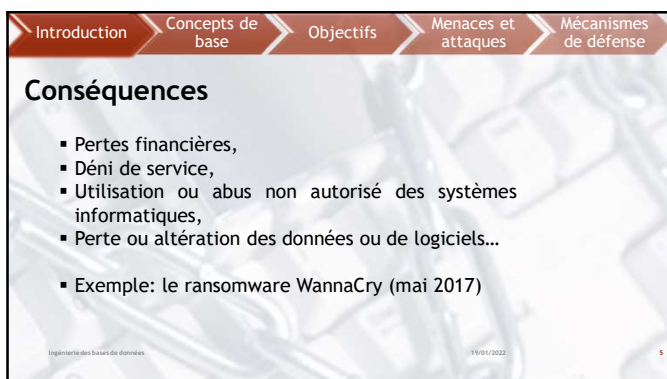
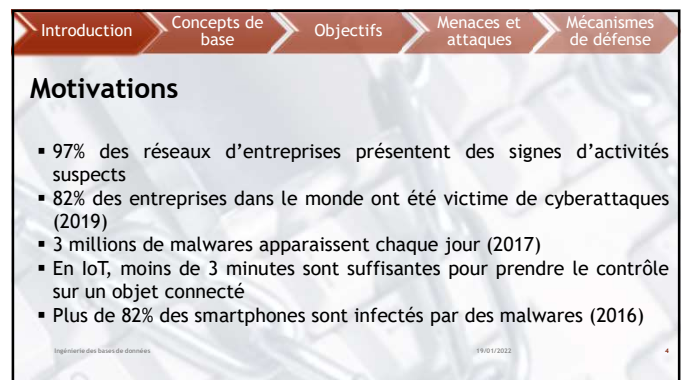
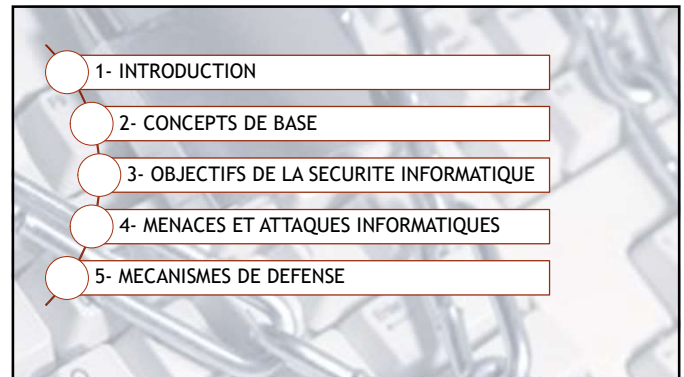
- Définir les objectifs de la sécurité informatique
- Etudier les concepts de base
- Identifier les mécanismes de défense
- Décrire des techniques d'attaques
- Simuler des attaques
- Cultiver l'esprit d'initiative et la volonté d'entreprendre
- Apprendre à déceler les risques liés aux différents changements et être capable d'anticiper

Langue d'enseignement :

☐ Arabe
 ☒ Français
 ☐ Anglais

Déroulement du cours

Semaine	Contenu	Références	Objectifs spécifiques
1	Présentation du cours Chapitre 1 : INTRODUCTION	(1) P4-P8	Définition de la sécurité informatique
2	Chapitre 2 : CONCEPTS DE BASE	(2) 9-12	Présenter les principaux concepts de la sécurité informatique
3	Chapitre 3 : OBJECTIFS DE LA SECURITE INFORMATIQUE	(3) 13- 20	Maitriser les principales propriétés de sécurité
4*	TP1: LES FONCTIONS DE HACHAGE	TP1	Manipuler les fonctions de hachage
5	TP1 (suite)	TP1	Simuler quelques attaques qui touchent à l'intégrité des données
6	Chapitre 4 : MENACES ET ATTAQUES INFORMATIQUE	(4) 21-32	Présenter les différents catégories et types d'attaques et de menaces informatique
	Chapitre 4 (Suite)		
7	Chapitre 5 : MECANISMES DE DEFENSES	(5) 33-40	Présenter de différents techniques et méthodes de défense
8	Devoir surveillé		
9	TP2: CHIFFREMENT SYMETRIQUE ET ASYMETRIQUE	TP2	Présenter la technique de chiffrement ainsi que ses 2 types
10	TD: CRYPTOSYSTEME D'ELGAMAL	TD1	
11	Chapitre 5 (suite)		
12	TP3: SIGNATURES ET CERTIFICATS NUMERIQUES	TP3	Présenter les techniques de signatures électroniques et certificats numériques
13	Semaine de préparation aux examens	Sujets des années antérieures	Être capable de résoudre les problèmes soulevés par ces sujets
14	Examen Final		



Introduction Concepts de base Objectifs Menaces et attaques Mécanismes de défense

Que couvre la sécurité en général?

- **Prévention**
 - Prendre des mesures afin d'empêcher les biens et les actifs d'être attaqués.
- **Détection**
 - Prendre des mesures afin de détecter quand, comment, par qui un actif ou un bien a été endommagé.
- **Réaction**
 - Prendre des mesures après un incident de sécurité afin de pouvoir restaurer les biens et les actifs, ou réduire l'impact de l'incident.

Ingenierie des bases de données 19/01/2022 7



CH 2
CONCEPTS DE BASE

Introduction Concepts de base Objectifs Menaces et attaques Mécanismes de défense

Menace

- Une menace est «un signe qui laisse prévoir un danger»
- La menace peut être une personne, un objet, ou un événement qui peut créer un danger pour un bien (en terme de confidentialité, intégrité ou disponibilité).
- Exemple:
 - Un virus circule sur le réseau local.
 - Un programme installé sur la machine semble être en train d'épuiser les ressources disponibles (mémoire, CPU).

Une attaque de sécurité est la réalisation d'une menace.

Ingenierie des bases de données 19/01/2022 9

Introduction Concepts de base Objectifs Menaces et attaques Mécanismes de défense

Vulnérabilité

- Faille ou bug pouvant être utilisé pour obtenir un niveau d'accès illicite à une ressource d'informations ou des privilèges supérieurs à ceux considérés comme normaux pour cette ressource.
- Une vulnérabilité est exploitée par une menace pour engendrer une attaque.
- Exemples de vulnérabilités :
 - Utilisation des mots de passe non robustes.
 - Présence de comptes non protégés par mot de passe.

Ingenierie des bases de données 19/01/2022 10

Introduction Concepts de base Objectifs Menaces et attaques Mécanismes de défense


Attaques

- Les moyens d'exploiter une vulnérabilité, on peut avoir plusieurs attaques pour une même vulnérabilité,

Contre-mesures

- Les procédures ou techniques permettant de résoudre une vulnérabilité ou de contrer une attaque spécifique

Ingenierie des bases de données 19/01/2022 11



CH 3
Objectifs

Introduction Concepts de base Objectifs Menaces et attaques Mécanismes de défense

Confidentialité

- Protection des données transmises contre les attaques passives, et protection des flux de données contre l'analyse.
- Préservation du secret des données transmises. Seulement les entités communicantes sont capables d'observer les données.
- Les algorithmes de chiffrement.

Ingénierie des bases de données 19/01/2022 13

Introduction Concepts de base Objectifs Menaces et attaques Mécanismes de défense

Intégrité

- Les données qui circulent sont bien celles que l'on croit
- Il n'y a pas eu d'altération au cours de la communication
- Doit valider l'intégralité des données, leur précision, l'authenticité et la validité:
 - Service orienté connexion: Protection contre la duplication, la destruction, l'insertion, la modification, le rejeu, le reclassement, etc.
 - Service non orienté connexion: Protection contre la modification uniquement.
- Fonctions de hachage.

Ingénierie des bases de données 19/01/2022 14

Introduction Concepts de base Objectifs Menaces et attaques Mécanismes de défense

Authentification

- S'assurer que l'origine du message soit correctement identifiée:
 - Assurer le receveur que le message émane de la source qui prétend avoir envoyé ce message.
 - Assurer l'authenticité des entités participantes: chacune des entités est celle qui prétend l'être.
 - Empêcher la perturbation de la connexion par une tierce partie qui se fait passer pour une entité légitime (émission ou réception non autorisée).

Utilisation de mot de passe, méthode de défi, secret partagé...

Ingénierie des bases de données 19/01/2022 15

Introduction Concepts de base Objectifs Menaces et attaques Mécanismes de défense

Non-répudiation

- La non-répudiation de l'information est la garantie qu'aucun des correspondants ne pourra nier la transaction
- Techniques utilisées: signature électronique

Ingénierie des bases de données 19/01/2022 16

Introduction Concepts de base Objectifs Menaces et attaques Mécanismes de défense

Disponibilité

- Elle exige l'accessibilité aux ressources à tout le temps défini de manière sécurisée et permanente. Et donc, on peut considérer comme une propriété d'un système informatique capable d'assurer ses fonctions sans interruption, délai ou dégradation, au moment même où la sollicitation en est faite ».
- Authentification, chiffrement...

Ingénierie des bases de données 19/01/2022 17

Introduction Concepts de base Objectifs Menaces et attaques Mécanismes de défense

Contrôle d'accès

- Empêcher l'utilisation non autorisée d'une ressource (serveur, application, etc.)
- Le service de contrôle d'accès doit :
 - Définir qui a le droit d'accéder aux ressources ?
 - Déterminer sous quelles conditions ceci peut avoir lieu ?
 - Définir ce qu'une entité est autorisée de faire lors de l'accès à une ressource.

Ingénierie des bases de données 19/01/2022 18

Introduction Concepts de base Objectifs Menaces et attaques Mécanismes de défense

Le modèle de sécurité AAA

A: Authentication
A: Authorization
A: Accounting

Ingénierie des bases de données 19/01/2022 19

101001010010001001000100010000001110101101
100100010010001000100011101010101110001001
10110010101110000100000010110
101000011010000100000000111011
101011001000000000000000000000
000001010000000000000000000000
011000100010111000110000110001
100110010000000000000000000000
111010010000000000000000000000
111000010000000000000000000000
101100010000000000000000000000
010100100100000000000000000000
001011000110100000000000000000
01101100001000000100111011010101101011

attack


CH 4
Menaces et attaques informatiques

Introduction Concepts de base Objectifs Menaces et attaques Mécanismes de défense

Catégories d'attaques

1) Interception

- C'est une attaque portée à la confidentialité,
- L'attaquant intercepte les paquets qui circulent sur un réseau




Ingénierie des bases de données 19/01/2022 21

Introduction Concepts de base Objectifs Menaces et attaques Mécanismes de défense

Catégories d'attaques:

2) Interruption

- C'est une attaque portée à la disponibilité,
- Rendre les services/les données d'un système inaccessibles




Ingénierie des bases de données 19/01/2022 22

Introduction Concepts de base Objectifs Menaces et attaques Mécanismes de défense

Catégories d'attaques:

3) Modification

- C'est une attaque portée à l'intégrité,
- Changer/altérer des données transmis sur un réseau




Ingénierie des bases de données 19/01/2022 23

Introduction Concepts de base Objectifs Menaces et attaques Mécanismes de défense

Catégories d'attaques:

4) Fabrication

- C'est une attaque portée à l'authenticité,
- Insertion de faux messages dans un réseau, ajout non-autorisé d'un enregistrement dans un fichier



Ingénierie des bases de données 19/01/2022 24

Introduction Concepts de base Objectifs Menaces et attaques Mécanismes de défense

Types d'attaques:

1) Attaques passives

- Ecouter sans modifier les données ou le fonctionnement du réseau,
- Capture du contenu d'un message et l'analyse de trafic,
- Généralement indétectables mais une prévention est possible

Ingénierie des bases de données 19/01/2022 25

Introduction Concepts de base Objectifs Menaces et attaques Mécanismes de défense

Types d'attaques:

2) Attaques actives

- Modifier, interrompre et/ou fabriquer des données: modification d'un flux de données ou création d'un flux frauduleux,
- Divisées en 4 catégories:
 - **Mascarade:** entité prétend être une autre entité (usurpation d'identité),
 - **Rejeu:** capture passive de données et retransmission,
 - **Modification de messages:** messages altérés, réorganisés ou retardés,
 - **Déni de service.**

Ingénierie des bases de données 19/01/2022 26

Introduction Concepts de base Objectifs Menaces et attaques Mécanismes de défense

Techniques d'attaques:

- Sniffing
- Spoofing
- Man in the Middle
- Denial of Service
- Spamming
- Phishing
- Cross-site scripting
- SQL injection
- etc.

Ingénierie des bases de données 19/01/2022 27

Introduction Concepts de base Objectifs Menaces et attaques Mécanismes de défense

Les menaces (malware)

- Le terme malware (*malicious software*) est utilisé pour désigner tout programme malveillant présent sur un ordinateur ou un appareil mobile.
- Peuvent générer des effets indésirables:
 - Paralysie des performances informatique,
 - Exploitation des données personnelles,
 - Suppression des données,
 - Etc.

Ingénierie des bases de données 19/01/2022 28

Introduction Concepts de base Objectifs Menaces et attaques Mécanismes de défense

Les menaces (malware)

Virus informatique

- La capacité à infecter plusieurs fichiers sur l'ordinateur,
- Se propagent vers les autres machines lorsque les fichiers infectés sont envoyés/transférés par e-mail ou sur des supports physiques (clé USB par exemple).

Ingénierie des bases de données 19/01/2022 29

Introduction Concepts de base Objectifs Menaces et attaques Mécanismes de défense

Les menaces (malware)

Vers (Worm)

- Ne nécessitent pas d'intervention humaine pour se propager,
- Il s'agit d'un programme capable d'utiliser des réseaux informatiques pour infecter les autres machines connectées, en exploitant les vulnérabilités du réseau,

Ingénierie des bases de données 19/01/2022 30

Introduction Concepts de base Objectifs Menaces et attaques Mécanismes de défense

Les menaces (malware)

- Rootkit,
- Enregistreur de frappe (Keylogger),
- Logiciel espion (spyware),
- Cheval de Troie (Trojan),
- Porte dérobée,
- Adware,
- Ransomware,
- Botnets,
- Minage de cryptomonnaie malveillant (Cryptojacking),

Ingénierie des bases de données 19/01/2022 31



CH 5
Mécanismes de défense

Introduction Concepts de base Objectifs Menaces et attaques Mécanismes de défense

Authentification

- Identifier et vérifier l'association entre l'utilisateur et son identité
- L'identité est une information unique associée à l'utilisateur, et connue du système d'authentification et de l'utilisateur,
- L'authentification sert à vérifier si un utilisateur ou une application a le droit de communiquer avec une autre application,
- Un service d'authentification se repose sur deux composantes:
 - L'identification: définir les identités
 - L'authentification: vérifier les identités

Ingénierie des bases de données 19/01/2022 33

Introduction Concepts de base Objectifs Menaces et attaques Mécanismes de défense

Contrôle d'accès

- La gestion des autorisation d'accès à des ressources: gérer et vérifier les droits d'accès, en fonction des règles de sécurité spécifiées dans la politique de sécurité,

Ingénierie des bases de données 19/01/2022 34

Introduction Concepts de base Objectifs Menaces et attaques Mécanismes de défense

Stéganographie

- C'est l'art de cacher un message secret au sein d'un autre message porteur (texte, image, son, vidéo...),
- La sécurité repose sur le fait que la présence d'un message secret ne sera pas détectée.
- Exemple: Collecter les mots de positions impairs:
Il ne faut pas tuer Jules César car il n'est pas le vrai coupable

Ingénierie des bases de données 19/01/2022 35

Introduction Concepts de base Objectifs Menaces et attaques Mécanismes de défense

Chiffrement

- Ensemble de techniques permettant de rendre incompréhensible des messages confidentiels,
- Le message initial est appelé **message en clair**,
- Après chiffrement, on obtient un **message chiffré**,
- Le chiffrement et le déchiffrement sont réalisés en se basant sur **des algorithmes**
- 2 types de chiffrement:
 - **Symétrique**: une seule clé partagée entre l'émetteur et le destinataire, appelée clé secrète ou privée,
 - **Asymétrique**: chaque entité communicante possède une paire de clés: clé publique et clé privée

Ingénierie des bases de données 19/01/2022 36

Introduction Concepts de base Objectifs Menaces et attaques Mécanismes de défense

Signature numérique

- C'est un mécanisme cryptographique utilisé pour vérifier l'authenticité d'un message,
- Une signature numérique peut être vue comme une version numérique des signatures manuscrites ordinaires, mais avec un niveau de sécurité accru,
- Sert de preuve que le message provient du bon émetteur,
- Permet d'assurer la non répudiation.

Ingénierie des bases de données 19/01/2022 37

Introduction Concepts de base Objectifs Menaces et attaques Mécanismes de défense

Fonctions de hachage

- Transformer des données de taille quelconque en une sortie de taille pré-déterminée,
- Tout changement dans les données d'entrée entraînerait une sortie complètement différente,
- La sortie est nommée hash ou empreinte,
- Les fonctions de hachage sont à sens unique: on ne peut retrouver le message d'origine à partir de son hash,
- Utilisées pour assurer l'intégrité des données.

Ingénierie des bases de données 19/01/2022 38

Introduction Concepts de base Objectifs Menaces et attaques Mécanismes de défense

Certification

- Un certificat numérique peut être vu comme une carte d'identité numérique,
- Les certificats numériques peuvent servir à l'authentification et à contrôler l'accès à certaines applications,

Ingénierie des bases de données 19/01/2022 39

Introduction à la Sécurité informatique

TP1 : Les fonctions de hashage

Pour se connecter à un compte sur un site web, une application ou tout autre service nécessitant une authentification, les mots de passe ne sont pas stockés directement dans un fichier. Le risque de fuite serait trop important.

Seul un *hash* de chaque mot de passe est enregistré sur un ordinateur : un *hash* est une suite de caractères de taille fixe associée à une chaîne quelconque.

- 1) Créer 3 fichiers qui contiennent :
 - i. Un texte en minuscule
 - ii. Le même texte en majuscule
 - iii. Un texte de taille différent que le premier
- 2) Générer les hashes de ces trois fichiers avec les fonctions de hashage suivantes :
 - i. Md5
 - ii. Sha1
 - iii. Sha256/sha512
- 3) Que remarquez-vous ?
- 4) Donnez les propriétés d'une fonction de hashage sécurisée
- 5) Expliquez pourquoi il n'est pas possible, même pour l'administrateur du serveur sur lequel les mots de passe sont enregistrés, de retrouver un mot de passe en cas de perte

Attaque par dictionnaire

Si on possède le hash d'un mot de passe, on peut essayer de retrouver le mot de passe en essayant toutes les possibilités.

En général, il est intéressant de commencer par les mots du dictionnaire.

- 6) Ecrivez un code qui permet de trouver le mot de passe ayant le hash suivant :

```
11f48731001d3a8e81b2305036b5cb2a19309d7fe86983e05fe16a2cb900e522
```

Pour ce faire, vous allez utiliser le fichier dic.txt qui contient les mots du dictionnaire "le Littré" qui ne contiennent pas d'accent. Il contient 47666 mots.

- 7) Combien de temps est-ce que la recherche prend ?

Attaque "brute force"

- 8) Ecrivez un code qui permet de tester tous les mots de passe d'une taille donnée (exemple taille=3).

- 9) Vérifiez que vous retrouvez bien le mot de passe de 3 lettres pour le hash

```
52a408a9e3ec559f30a16ca8baf40761c9607e8755f63599957de2f6412a0005
```

- 10) Combien de temps est-ce que cela prend ?

- 11) Modifiez le programme pour qu'il teste tous les mots de passe de 4 lettres, et recherchez le mot de passe pour le hash

```
e13b5b56520b1aa82029053158f2b017816a4e9618da08e82703c05a9d8628c1
```

- 12) Combien de temps est-ce que cela prend ?

- 13) Modifiez le programme pour qu'il teste tous les mots de passe de 5 lettres, et recherchez le mot de passe pour le hash

```
7fd2e09b9e362ece70e60489dd8a082ea6118cbdae94a7866e9617c3deab0939
```

- 14) Combien de temps est-ce que cela prend ?

Introduction à la sécurité informatique**TP2 P : Chiffrement****Introduction**

Ce TP a pour objectif de se familiariser avec les notions liées à la cryptographie. Il s'articule autour de deux parties : Dans la première partie, vous serez amenés à utiliser la méthode de chiffrement symétrique des messages et vérifier la rapidité de cette méthode ainsi que ses inconvénients. La deuxième partie traitera l'utilisation des chiffrements asymétriques, la lourdeur de cette méthode ainsi que ses avantages. Le logiciel GPG (gardien de la vie privée) <https://gnupg.org> est la version GNU de PGP (Pretty Good Privacy) <https://openpgp.org>

Partie 1 : Chiffrement symétrique

- (a) En utilisant la commande "man gpg", essayez de parcourir l'aide de notre logiciel.
- (b) Dans un répertoire TP2, créer un fichier texte contenant le message suivant : "Bonjour les gars !". Exécuter les commandes suivantes :

- "gpg --symmetric nom_fichier" :
- "gpg --symmetric --armor nom_fichier" :

Vérifiez l'output de ces deux commandes, Que remarquez-vous ?

- (c) Décrypter le fichier chiffré en utilisant la commande "gpg --decrypt nomFichiergénéré".

Quel est le résultat de l'exécution ? Quel algorithme de chiffrement a été utilisé ?

- (d) Pour garantir l'intégrité des messages, vous allez utiliser une fonction de hachage H() de votre choix. Pour ce faire :

i. Echanger ce tuple (H(fichier), fichier.asc, le nom de la fonction de hachage utilisée, un Random) en utilisant Secure Shell avec votre camarade.

- ii. Si vous avez la clef de déchiffrement, procédez au déchiffrement et vérifiez l'intégrité de votre fichier.
- iii. Pour prouver à votre expéditeur la bonne réception du message, envoyez-lui une incrémentation de votre random, plus votre identité (votre nom par exemple).
- iv. Changez légèrement le déchiffré du fichier et vérifiez la détection de la fraude.
- v. Enumérez les inconvénients du chiffrement symétrique, et comment y remédier ?

Partie 2 : Chiffrement asymétrique

- (a) Générez une paire de clé avec la commande `gpg --gen-key` en utilisant les paramètres par défaut.
- (b) Listez votre trousseau de clés avec la commande `gpg --list-keys` et validez la présence de vos clés.
- (c) Exportez votre clé publique avec la commande `gpg --armor --output maclé.asc --export UserID` et donnez le résultat.

UserID est l'identité (l'adresse email par exemple) de la clé concernée.

- (d) Créez un fichier texte contenant un petit paragraphe, et chiffrez ce document avec la commande `gpg -er UserID document.txt`. Validez le résultat en visualisant le fichier `document.txt.gpg`, et supprimez le document non chiffré.
- (e) Déchiffrez le document chiffré créé précédemment avec la commande `gpg document.txt.gpg`, et validez le résultat.
- (f) Signez le document texte initial avec la commande `gpg --clearsign document.txt`. Validez le résultat en visualisant le fichier `document.txt.asc`.
- (g) Vérifiez le document signé avec la commande `gpg --verify document.txt.asc`.
- (h) Quelle est l'utilité de la signature numérique ?

Introduction à la sécurité informatique**TD1 : Chiffrement asymétrique : cryptosystème d'El-Gamal**

La sécurité de la méthode de chiffrement asymétrique d'ElGamal repose sur la difficulté de calculer les logarithmes discrets (le problème du logarithme discret consiste à retrouver un entier s tel que $h = g^s \bmod p$, il y a beaucoup de possibilité de s).

- Les paramètres publics :
 - q un nombre premier (exemple : $q=5$).
 - $p = 2q + 1$ un nombre premier (exemple : $p=11$).
 - G_q un sous-groupe de Z_p^* d'ordre q .
 - g un générateur de G_q .
- La clef secrète de l'utilisateur $x \in G_q$
- La clef publique de cet utilisateur $y = g^x \bmod p$

Chiffrement

Soit m un message en clair :

- 1) Choisir un nombre aléatoire $k \in G_q$,
- 2) Calculer $(u = g^k \bmod p, v = y^k m \bmod p)$,
- 3) Envoyer le couple $(u,v) = E_{g,y}(m)$

Déchiffrement

$$D_x(u,v) = v/u^x$$

Exercice 1

Le codage de $A = 01$, celui de $B = 02$, et ainsi de suite jusqu'à $Z = 26$. Un mot comme *Crypto* son encodage donne 031825162015=31825162015.

Soient les paramètres du cryptosystème ElGamal dans \mathbb{F}_p :

$$p = 150001$$

$$g = 7$$

$$a = 113$$

$$k = 1000$$

p un nombre premier.

g le générateur du groupe G_q , avec G_q un sous groupe de Z_p^* .

a est la clef privée.

$k \in_R G_q$

1. Calculer la clef publique (p, g, A) . Avec A la clef complémentaire de a .
2. Soit le message "Hi Men", Crypter ce message avec la clef publique (p, g, A) .
3. Vérifier le message chiffré en le décryptant et retrouvant les messages d'origine.

Exercice 2

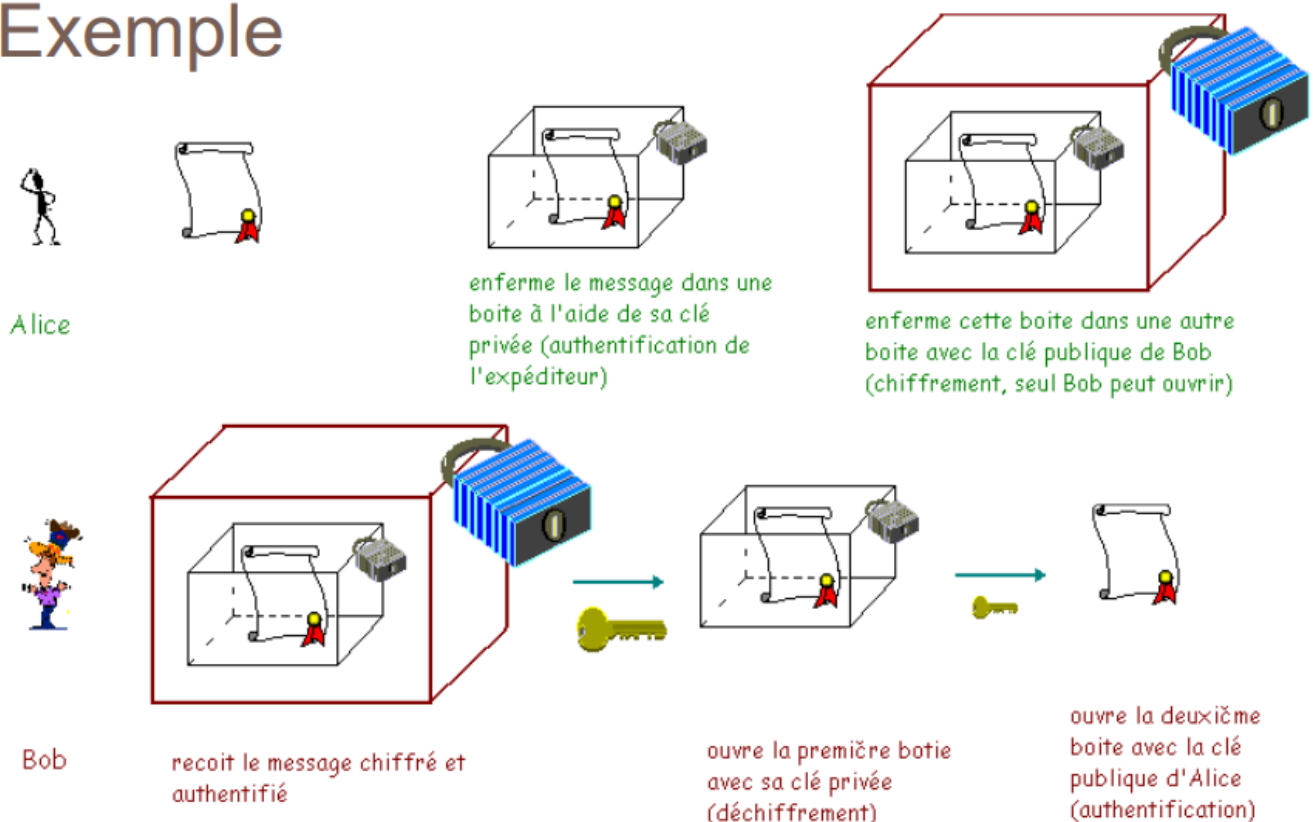
1. Soient $p = 541$, $g = 2$, $a = 113$ et $k = 101$. Crypter $x = 200$ et $x = 201$ en utilisant le cryptosystème ElGamal.
2. Soient $p = 541$, $g = 2$, $a = 101$. Décrypter les chiffrés du cryptosystème ElGamal $y = (54, 300)$ et $y = (54, 301)$

Introduction à la sécurité informatique

TP3 : OpenSSL : les certificats numériques

Comment être sûr de l'expéditeur ?

Exemple

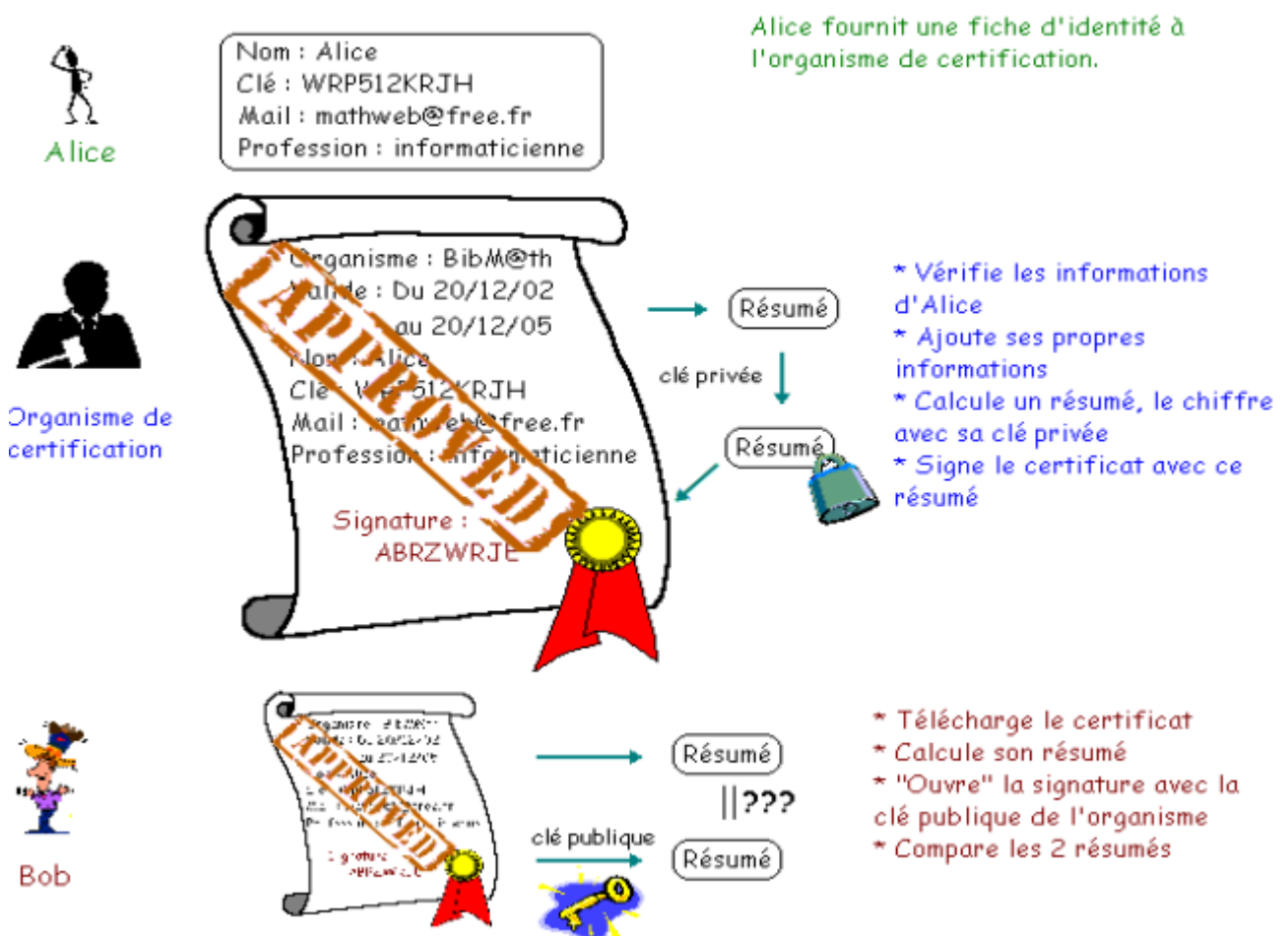


Comme dans la vie courante, on a recours à des certificats :

- Pour passer un examen, il vous faut prouver votre identité : fournir une carte d'identité, passeport ou permis de conduire.
- Un organisme supérieur (l'Etat) a signé ces certificats, s'assurant auparavant (par un acte de naissance...) qu'il s'agit bien de vous.

Les certificats numériques fonctionnent sur le même principe (Figure ci-dessous):

- Alice veut certifier que sa clé publique lui appartient. Elle envoie sa clé à un organisme de certification, ainsi que différentes informations la concernant (nom, email, etc...).
- Cet organisme vérifie les informations fournies par Alice, et ajoute au certificat son propre nom, une date limite de validité, et surtout une signature numérique.
- Cette signature est calculée de la façon suivante : à partir des informations du certificat, l'organisme calcule un résumé en appliquant une fonction de hachage connue, comme MD5. Puis il signe ce résumé en lui appliquant sa clé secrète.



Ce TP a pour objectif de faire le premier pas avec les certificats "X509". On va se focaliser sur les certificats auto-signé. Un certificat auto-signé est comme le certificat de l'autorité de certification "root" qui va signer lui-même son certificat. Théoriquement, ça n'a pas de valeur, mais ici, c'est nous le tiers de confiance et nous savons qui nous sommes.

1. Etape1 : Création du certificat de l'autorité de certification

(a) Pour signer un certificat, vous devez devenir votre propre autorité de certification, cela nécessite la génération d'une paire de clef et d'un certificat auto-signé.

(b) La création de la clef privée de l'autorité de certification se fait de la manière suivante:

« ***openssl genrsa -out CLEF_auth -des3 4092*** ».

L'option -des3 introduit l'usage d'une "passphrase", cette "passphrase" sera demandée à chaque appel de la CLEF_auth.

(c) A partir de CLEF_auth, on crée un certificat x509 pour une durée de validité de 10 ans :

« ***openssl req -new -x509 -days 3650 -key CLEF_auth -out ANCE_cert*** ».

(d) Remplissez les divers champs en simulant l'autorité de votre pays. Dans notre cas de figure, la CA est la ANCE. Le champs *common name* représente le site de votre autorité (ANCE.tn).

(e) Le résultat obtenu est le certificat d'autorité de certification qui va permettre de signer les certificats créés.

2. Etape2 : Génération d'une demande de signature d'un certificat à un serveur

(a) On génère la clef privée CLEF_serv avec les commandes précédentes.

(b) Ensuite, on lance une demande de signature de certificat (CSR Certificate Signing Request) avec la commande suivante :

« ***openssl req -new -key CLEF_serv -out demande_serveur*** ».

Comme précédemment, remplissez tous les champs de la demande de votre serveur.

3. Etape3 : La signature de la demande du serveur par le CA (Certificate Authority)

(a) La commande qui signe la demande de certificat est la suivante :

« openssl x509 -req -in demande_serveur -out serveur_cert -CA ANCE_cert -CAkey CLEF_auth -CAcreateserial -CAserial serveur.srl ».

L'option CAcreateserial n'est nécessaire que la première fois. Le certificat signé est le fichier "serveur_cert".

(b) Pour vérifier le certificat généré, il est nécessaire de disposer du certificat de l'autorité qui l'a émis :

« openssl verify -CAfile ANCE_cert serveur_cert »

(c) Pour pouvoir exporter le certificat dans le magasin du navigateur, il faut le convertir en extension PKCS12 certificate et le résultat est la combinaison du fichier certificat/clef :

« openssl pkcs12 -export -out serveur_cert.pfx -in serveur_cert -inkey CLEF_serv -name "Certificate of server" »

(d) Une fois le certificat « serveur_cert.pfx » uploadé, remarquez que ce certificat n'est pas vérifié par votre navigateur.

(e) Pour valider cette vérification, uploader le certificat de l'autorité de certification dans le navigateur. C'est ce dernier qui va valider le certificat du serveur "serveur_cert.pfx".

4. Etape4 : Affichage des informations contenues dans un certificat

(a) Le certificat du serveur

« openssl x509 -in serveur_cert -text -noout »,

Remarquez la présence de qui a émis le certificat et pour qui.

(b) Qui a émis le certificat ?

« openssl x509 -noout -in serveur_cert -issuer »

(c) Pour qui a-t-il été émis ?

« openssl x509 -noout -in serveur_cert -subject »

(d) Quelle est sa période de validité ?

« openssl x509 -noout -in serveur_cert -dates »

(e) Toutes les infos précédentes :

« *openssl x509 -noout -in serveur_cert -issuer -subject -dates* »

(f) Quelle est sa valeur de hachage ?

« *openssl x509 -noout -in serveur_cert -hash* »

(g) Quelle est son empreinte ?

« *openssl x509 -noout -in serveur_cert -fingerprint* »