Université: Badji Mokhtar Annaba **Semestre:** 02
Niveau: L3 **Année:** 2024/2025

Module: Sécurité Informatique

Série TD 1

Question 1 : Imaginez un monde sans sécurité informatique. Quels seraient les impacts sur la vie quotidienne des individus, des entreprises et des États ?

À partir de cette réflexion, quels sont les principaux motivations qui justifient la nécessité de la sécurité informatique ?

Question 2 : Déterminez si chaque incident relève de la sécurité interne ou externe, puis proposez une solution efficace pour éviter qu'il ne se reproduise à l'avenir.

1. Un employé télécharge par erreur un logiciel infecté depuis son ordinateur professionnel
2. Un hacker tente d'arrêter la plateforme d'une entreprise via une attaque de déni de service distribué (DDoS).
3. Un mot de passe faible d'un cadre supérieur est piraté et utilisé pour accéder aux données confidentielles.
4. Un e-mail frauduleux (phishing) cible plusieurs employés pour voler leurs identifiants.
5. Un technicien en interne copie des fichiers sensibles sans autorisation.
6. Un employé perd son ordinateur portable professionnel contenant des données sensibles

Question 3 : Analyses des risques et préjudices

1. Expliquez avec vos propres mots les concepts suivants en sécurité informatique : **vulnérabilité, menace, attaque, préjudice, probabilité et risque**.
2. Illustrer votre explication avec un exemple concret lié à une **injection SQL**, en tenant compte du fait que vous devez concevoir un site web ou une application.
3. **Calcul :** Si la probabilité d'une attaque est de 30 % et que le préjudice potentiel est estimé à 100 000 €, quel est le risque associé ? Utilisez la formule d'estimation du risque.

Question 4 : Politiques de sécurité

1. Qu'est-ce qu'une politique de sécurité et quels sont ses objectifs ?
2. Associez chaque scénario ci-dessous à l'objectif de sécurité qu'il compromet :
   a. Un serveur tombe en panne, rendant les données inaccessibles pendant plusieurs heures (……)
   b. Un acteur malveillant accède à une base de données client en exploitant une faille de sécurité (……)
   c. Un virus altère des fichiers critiques sur un serveur.
   d. Un threat actor utilise les identifiants volés d'un employé pour accéder au réseau de l'entreprise (……)
   e. Une transaction financière est effectuée, mais aucun enregistrement de l'utilisateur ne peut en attester (……)
   f. Un client nie avoir passé une commande en ligne, alors que le système prouve le contraire (……)
   g. Un fichier confidentiel est modifié en transit par un attaquant (……)
   h. Une panne de serveur entraîne une perte de données, et il est impossible d'en identifier la cause exacte (……)

3. Quelle est la différence entre un pare-feu (Firewall), un système de détection d'intrusion (IDS) et un système de prévention d'intrusion (IPS) dans la mise en œuvre d'une politique de sécurité ?

Question 5 : Attaques et contre-mesures

1. Quelle est la différence entre une attaque passive et une attaque active ? Donnez un exemple pour chaque type.
2. Complétez le tableau suivant en associant chaque type d'attaque à sa catégorie, sa description et un exemple :

Type d'attaque	Catégorie	Description	Exemple
Interception			
Interruption			
Modification			
Fabrication			

Question 6 : La norme ISO 27000

1. Quel est l'objectif principal de la norme ISO 27000 ?
2. Quelles sont les principales normes de la famille ISO 27000 et quel est le rôle de chaque norme?
3. Quelles sont les quatre phases de la norme ISO 27000 et quel est l'objectif de chaque phase.

Université: Badji Mokhtar Annaba **Semestre:** 02
Niveau: L3 **Année:** 2024/2025

Module: Sécurité Informatique

Série TD 1

Question 1 : Imaginez un monde sans sécurité informatique. Quels seraient les impacts sur la vie quotidienne des individus, des entreprises et des États ?

À partir de cette réflexion, quels sont les principaux motivations qui justifient la nécessité de la sécurité informatique ?

(Dans le cours, première page)

Question 2 : Déterminez si chaque incident relève de la sécurité interne ou externe, puis proposez une solution efficace pour éviter qu'il ne se reproduise à l'avenir.

1. Un employé télécharge par erreur un logiciel infecté depuis son ordinateur professionnel
2. Un hacker tente d'arrêter la plateforme d'une entreprise via une attaque de déni de service distribué (DDoS).
3. Un mot de passe faible d'un cadre supérieur est piraté et utilisé pour accéder aux données confidentielles.
4. Un e-mail frauduleux (phishing) cible plusieurs employés pour voler leurs identifiants.
5. Un technicien en interne copie des fichiers sensibles sans autorisation.
6. Un employé perd son ordinateur portable professionnel contenant des données sensibles

	Scénario	Notions à discuter	Type de sécurité	Solution
1	Un employé télécharge par erreur un logiciel infecté depuis son ordinateur professionnel.	/	Interne	Formation des employés sur la cybersécurité + Mise en place d'un système de restriction des téléchargements.
2	Un hacker tente de pénétrer votre réseau via une attaque par déni de service (DDoS).	DoS, How it works + DDoS	Externe	Utilisation d'une protection anti-DDoS et d'un pare-feu avancé.
3	Un mot de passe faible d'un cadre supérieur est piraté et utilisé pour accéder aux données confidentielles.	Brute force	Interne	Imposition de mots de passe forts + Activation de l'authentification à deux facteurs (2FA).
4	Un e-mail frauduleux (phishing) cible plusieurs employés pour voler leurs identifiants.	Phishing	Externe	Filtrage des e-mails + Sensibilisation des employés au phishing.
5	Un technicien en interne copie des fichiers sensibles sans autorisation.	Gestion d'accès	Interne	Surveillance des accès aux fichiers + Mise en place d'une gestion stricte des autorisations.
6	Un employé perd son ordinateur portable professionnel Contenant des données sensibles	\	Interne	Les données sensibles doivent être stockées dans un endroit (serveur) sécurisé (sécurité physique)

Question 3 : Analyses des risques et préjudices

1. Expliquez avec vos propres mots les concepts suivants en sécurité informatique : **vulnérabilité, menace, attaque, préjudice, probabilité et risque**.

Une **vulnérabilité** est une faiblesse ou une faille dans un système, un logiciel, un réseau ou un processus qui pourrait être exploitée par une menace.

Une **menace** est tout élément ou événement susceptible d'exploiter une vulnérabilité et de causer un dommage. Une menace peut être intentionnelle (pirate informatique) ou accidentelle (erreur humaine, catastrophe naturelle).

Une **attaque** est l'action concrète menée par une menace pour exploiter une vulnérabilité. Elle peut être technique (virus, phishing, injection SQL) ou sociale (ingénierie sociale).

Le **préjudice** est l'impact négatif causé par une attaque réussie. Cela peut être une perte financière, une atteinte à la réputation, une violation de données, etc.

La **probabilité** est la mesure du risque qu'une menace exploite une vulnérabilité. Plus une faille est facile à exploiter, plus la probabilité d'une attaque est élevée.

Le **risque** est le résultat de la combinaison entre une vulnérabilité, une menace, et la probabilité d'exploitation, menant à un préjudice.

2. Illustrer votre explication avec un exemple concret lié à une **injection SQL**, en tenant compte du fait que vous devez concevoir un site web ou une application.

L'injection SQL : est une attaque qui exploite une faille dans une application pour injecter du code SQL malveillant, permettant d'accéder, modifier ou supprimer des données dans une base de données.

Exemple d'une requête ordinaire :

```
SELECT * FROM utilisateurs WHERE username = '$input' AND password = '$password';
```

Un attaquant peut entrer :

```
' OR 1=1 --
```

Ce qui transforme la requête en :

```
SELECT * FROM utilisateurs WHERE username = '' OR 1=1 --' AND password = '';
```

Cela donne accès à tous les comptes.

Illustrer votre explication avec un exemple concret lié à une **injection SQL :**

- **Vulnérabilité** : Formulaire acceptant des entrées utilisateur sans filtrage ni requêtes préparées.
- **Menace** : Un attaquant tente d'exploiter cette faille pour accéder aux données.
- **Attaque** : L'attaquant injecte du code SQL (`' OR 1=1 --`) pour contourner l'authentification.
- **Préjudice** : Vol ou suppression des données, compromission des comptes utilisateurs.
- **Probabilité** : Élevée si aucune protection n'est mise en place.
- **Risque** : Critique si l'application contient des données sensibles et qu'aucune mesure de sécurité n'est appliquée.

3. **Calcul :** Si la probabilité d'une attaque est de 30 % et que le préjudice potentiel est estimé à 100 000 €, quel est le risque associé ? Utilisez la formule d'estimation du risque.

Formule : Le risque = préjudice *Probabilité de production

Données :

Probabilité d'attaque = 30 % = 0.30

Préjudice potentiel = 100 000 €

Calcul :

Risque = 0.30 × 100000 €

Risque = 30000 €

Interprétation :

Le risque estimé est 30 000 €. Cela signifie qu'en moyenne, l'impact financier attendu de cette attaque est de 30 000 €, ce qui justifie la mise en place de mesures de sécurité pour réduire soit la probabilité d'attaque, soit le préjudice potentiel.

Question 4 : Politiques de sécurité

1. Qu'est-ce qu'une politique de sécurité et quels sont ses objectifs ?

(Def dans le cours : Une politique de sécurité est un ensemble de règles, de procédures et de bonnes pratiques mises en place pour protéger les systèmes informatiques, les données et les utilisateurs contre les menaces et les risques de sécurité

Objectifs : Disponibilité, Confidentialité, Intégrité, Authentification, Traçabilité, Non-répudiation)

2. Associez chaque scénario ci-dessous à l'objectif de sécurité qu'il compromet :
   a. Un serveur tombe en panne, rendant les données inaccessibles pendant plusieurs heures (Disponibilité)
   b. Un acteur malveillant accède à une base de données client en exploitant une faille de sécurité (Confidentialité)
   c. Un virus altère des fichiers critiques sur un serveur (Intégrité)
   d. Un threat actor utilise les identifiants volés d'un employé pour accéder au réseau de l'entreprise (Authentification)
   e. Une transaction financière est effectuée, mais aucun enregistrement de l'utilisateur ne peut en attester (Traçabilité)
   f. Un client nie avoir passé une commande en ligne, alors que le système prouve le contraire (Non-répudiation)
   g. Un fichier confidentiel est modifié en transit par un attaquant (Confidentialité et Intégrité)
   h. Une panne de serveur entraîne une perte de données, et il est impossible d'en identifier la cause exacte (Disponibilité et Traçabilité)
3. Quelle est la différence entre un pare-feu (Firewall), un système de détection d'intrusion (IDS) et un système de prévention d'intrusion (IPS) dans la mise en œuvre d'une politique de sécurité ?

   Pare-feu (Firewall) : Filtre le trafic réseau en appliquant des règles de sécurité pour autoriser ou bloquer les connexions. Il agit comme une barrière entre un réseau sécurisé et un réseau non fiable.

Système de détection d'intrusion (IDS) : Surveille les logs (réseau, système, ..) qui dépasse le Firewall et détecte les activités suspectes ou malveillantes, mais il n'intervient pas directement pour bloquer les attaques.

Système de prévention d'intrusion (IPS) : Fonctionne comme un IDS, mais avec la capacité de bloquer ou neutraliser automatiquement les menaces détectées en temps réel.

Question 5 : Attaques et contre-mesures

1. Quelle est la différence entre une attaque passive et une attaque active ? Donnez un exemple pour chaque type.

Attaque passive : L'attaquant espionne les communications ou collecte des informations sans modifier les données ni perturber le système. L'objectif est la surveillance ou l'exfiltration d'informations.
Exemple : L'écoute clandestine d'un trafic réseau (sniffing) pour capturer des identifiants de connexion.

Attaque active : L'attaquant modifie, altère ou interrompt les communications ou les données pour causer des dommages ou obtenir un avantage.
Exemple : Une injection SQL permettant à un attaquant de modifier ou supprimer des données d'une base.

2. Complétez le tableau suivant en associant chaque type d'attaque à sa catégorie, sa description et un exemple :

Type d'attaque	Catégorie	Description	Exemple
Interception	Passive	Dans le cours	Sniffing
Interruption	Active	//	ARP Poisoning
Modification	Active	//	Man in the middle (MiTM)
Fabrication	Active	//	DDoS

Question 6 : La norme ISO 27000

1. Quel est l'objectif principal de la norme ISO 27000 ?
2. Quelles sont les principales normes de la famille ISO 27000 et quel est le rôle de chaque norme?
3. Quelles sont les quatre phases de la norme ISO 27000 et quel est l'objectif de chaque phase.

Sécurité informatique

Série 2 : Initiation à la cryptographie (César / Transposition)

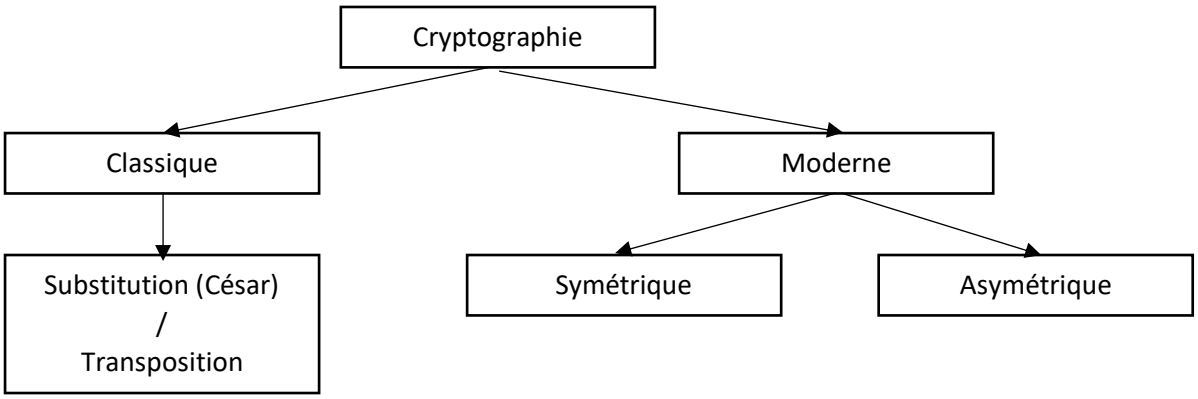
« *La cryptographie est l'art et la science de sécuriser les communications en transformant des informations en un format illisible pour toute personne non autorisée, puis en les rendant lisibles uniquement pour ceux qui possèdent la clé de déchiffrement appropriée.* »

1. Objectifs de la Cryptographie ?

2. Principaux Concepts :

- Chiffrement
- Déchiffrement
- Clé
- Algorithme
- Cryptanalyse

3. Types de Cryptographie :



Exercice 1 : (Algorithme de César)

1.1. Chiffrement avec l'algorithme de César

Chiffrez le message suivant en utilisant l'algorithme de César avec un décalage de 3 lettres :
Message clair : "BONJOUR"

1.2. Déchiffrement avec l'algorithme de César

Déchiffrez le message suivant qui a été chiffré avec l'algorithme de César avec un décalage de 5 lettres :
Message chiffré : "GFION RTPMYFW"

1.3. Déchiffrement sans clé avec l'algorithme de César

Déchiffrez le message suivant qui a été chiffré avec l'algorithme de César sans connaître le décalage :
Message chiffré : "HUUHIH"

Exercice 2 : (Algorithme de chiffrement par transposition)

Par exemple, en utilisant la clé k = 164325

Le message clair M =« MESSAGE SECRET A CHIFFRER PAR TRANSPOSITION »,

Nous obtenant le cryptogramme C =« METFRPO ARIPNT SCHRAI SECERS GEFASI ESARTON »

Chiffrement	Déchiffrement
1. Calculer le nombre de caractères du message clair M. 2. Préparation de la matrice : a. Colonnes (selon la clé) b. Lignes (Nb.M / Nb.Cle) 3. Remplissage par Lignes 4. Écrire le message par Colonnes selon la clé	1. Calculer le nombre de caractères du message Chiffré C. 2. Préparation de la matrice : a. Colonnes (selon la clé) -6- b. Lignes (Nb.M / Nb.Cle) 6+6+ … + 2 3. Remplir le message C par Colonnes selon la clé 4. Écrire le message M Par lignes

2.1. Quel est le cryptogramme C correspondant au texte clair M = « MATHEMATIQUES ET INFORMATIQUE » et la clé k = « 356124 » ?

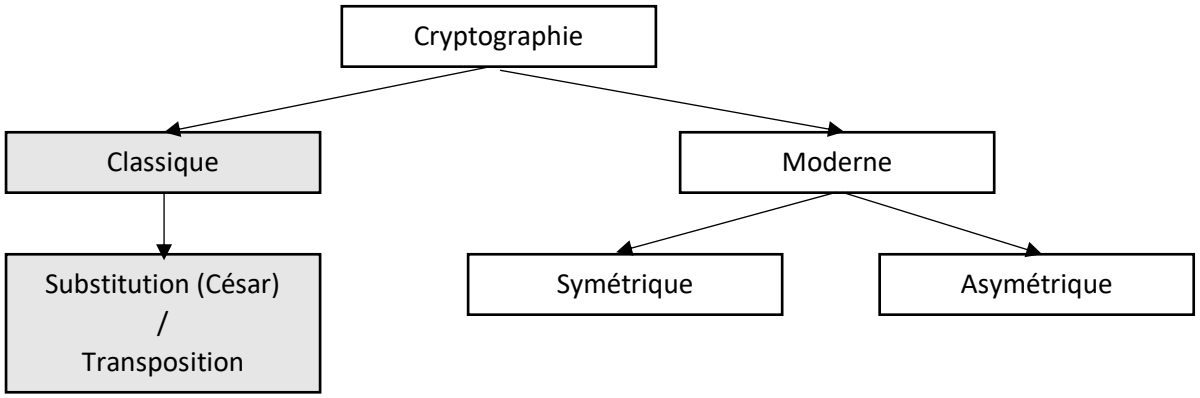
2.2. Quel est le texte clair M correspondant au cryptogramme C «USCCLSETFEIESTCSEADEXCENA » et la clé k = « 356124 » ?

TD Sécurité Informatique

Série TD 3.1 : *Cryptographie Symétrique (S-DES)*

Rappel :

- Série 1 : Service, Menaces, Mécanismes, ISO 27002
- Série 2 : Cryptographie classique (César, Transposition)



Cryptographie Symétrique (S-DES) :

1. Quelle est la différence entre la cryptographie symétrique et asymétrique ?
2. Comment les deux parties communicantes s'échangent-elles la clé secrète dans le contexte de la cryptographie symétrique afin de garantir la confidentialité des données échangées ?
3. Liste des algorithmes de chiffrement symétrique les plus connus :
   - AES (Advanced Encryption Standard)
   - ~~DES (Data Encryption Standard)~~
   - 3DES (Triple Data Encryption Standard)

4. Quelle est la différence fondamentale entre l'algorithme **S-DES** (Simplified Data Encryption Standard) et le **DES** (Data Encryption Standard) complet ?

S-DES or Simplified Data Encryption Standard

1. S-DES chiffre des blocs de **8 bits**.
2. La **clé** de chiffrement est de **10 bits**.
3. Deux tours de chiffrement.

Exemple :

Trouvez les valeurs de K1, K2, et le texte chiffré en utilisant l'algorithme S-DES avec les paramètres suivants :

- Clé: 10111 00111 -> K1: 1011 1110 / K2: 1101 1011
- Plain text: 0110 1100

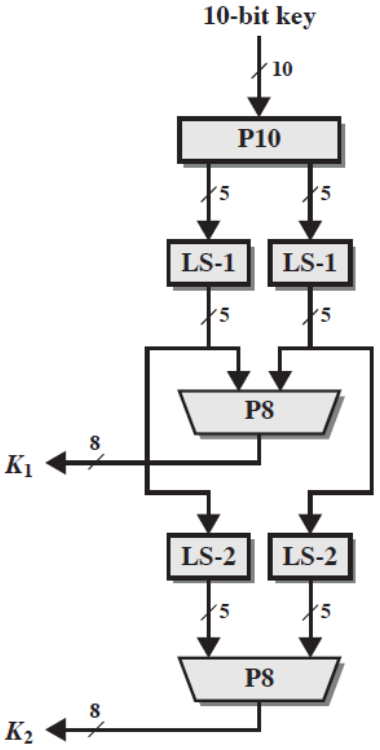
Exercise 01:

Trouvez les valeurs de K1, K2, et le texte chiffré en utilisant l'algorithme S-DES avec les paramètres suivants :

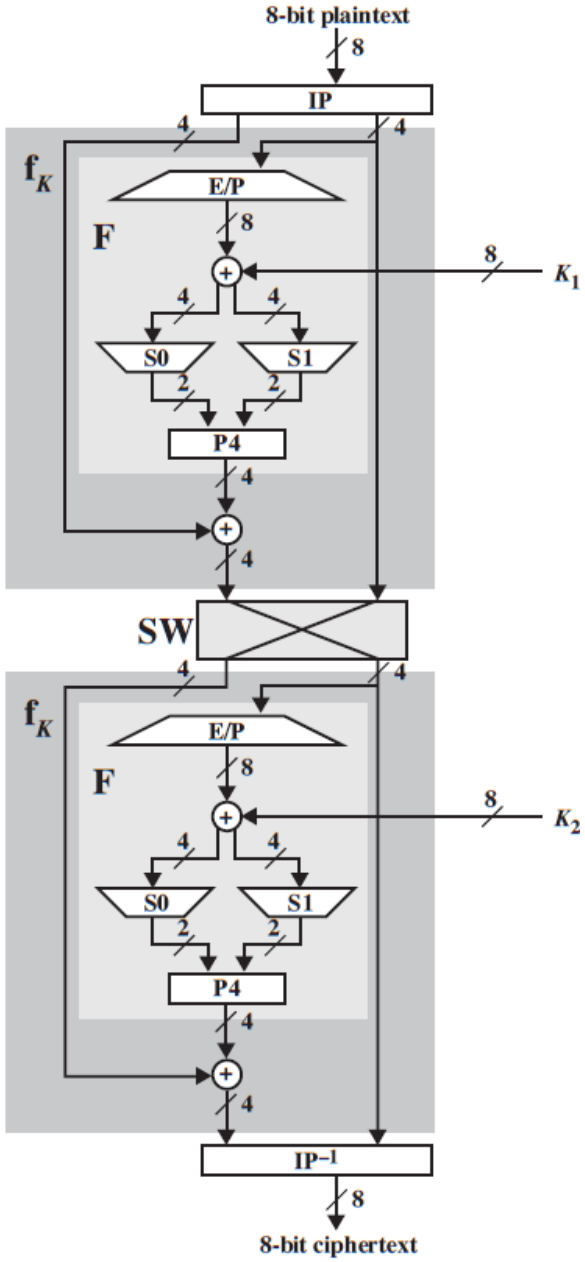
- Clé : 10100 00010
- Texte Clair (r): 0111 0010

Indiquez clairement vos calculs pour chaque étape.

1. Génération des Clés



2. Chiffrement



Permutations (inchangeable)

P 10									
3	5	2	7	4	10	1	9	8	6

P 8							
6	3	7	4	8	5	10	9

IP							
2	6	3	1	4	8	5	7

IP^{-1}							
4	1	3	5	7	2	8	6

E/P							
4	1	2	3	2	3	4	1

P4			
2	4	3	1

$$S0 = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{cccc} 0 & 1 & 2 & 3 \end{array} \\ \begin{bmatrix} 1 & 0 & 3 & 2 \\ 3 & 2 & 1 & 0 \\ 0 & 2 & 1 & 3 \\ 3 & 1 & 3 & 2 \end{bmatrix} \end{array} \qquad S1 = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{cccc} 0 & 1 & 2 & 3 \end{array} \\ \begin{bmatrix} 0 & 1 & 2 & 3 \\ 2 & 0 & 1 & 3 \\ 3 & 0 & 1 & 0 \\ 2 & 1 & 0 & 3 \end{bmatrix} \end{array}$$

TD Sécurité Informatique

Série TD 3.2 : Cryptographie Asymétrique (RSA)

À votre avis, quelles sont les **limites** de la cryptographie symétrique ?

Cryptographie asymétrique : L'algorithme RSA

L'algorithme RSA est un algorithme de cryptographie asymétrique largement utilisé. RSA a été publié pour la première fois en 1977 par Ron Rivest, Adi Shamir et Leonard Adleman, d'où son nom RSA (Rivest-Shamir-Adleman).

1. Chaque utilisateur possède deux clés : une clé publique et une clé privée.
2. La clé privée doit être stockée de manière sécurisée et ne doit jamais être divulguée à quiconque.
3. Il est impossible de déduire une clé à partir de l'autre, car elles sont générées à l'aide de formules mathématiques irréversibles.
4. Si vous chiffrez un message avec l'une des clés, vous pouvez le déchiffrer avec l'autre clé correspondante.

RSA : Mode de Fonctionnement

Phase 1 : Génération des clés (publique et privée)

1. **Choisir deux nombres premiers distincts :** Choisissez deux nombres premiers distincts ***p*** et ***q***. Ces nombres doivent être suffisamment grands pour assurer la sécurité du système. Plus ces nombres sont grands, plus la sécurité est renforcée. *(P=3, Q=11)*

2. **Calculer *n* :** Calculez le produit des deux nombres premiers : $n = p \times q$.

3. **Calculer la fonction d'Euler $\phi(n)$:** Calculer la fonction d'Euler de ***n***, qui est le nombre d'entiers positifs inférieurs à ***n*** qui sont premiers avec ***n***. Pour deux nombres premiers distincts ***p*** et ***q***, $\phi(n) = (p-1)\times(q-1)$.

4. **Choisir *l'exposant de chiffrement public* (e):** Sélectionnez un entier ***e*** tel que $1<e<\phi(n)$ et ***e*** est premier avec $\phi(n)$. ***e*** est généralement choisi petit.

5. **Calculer l'exposant de déchiffrement privé (*d*) :** en utilisons l'algorithme d'Euclide étendu, calculez l'exposant de déchiffrement ***d*** : $d \times e \equiv 1 \bmod \phi(n)$

6. **Clés générées :** Les clés publiques sont **(*n*, *e*)** et la clé privée est ***d***.

Une fois que vous avez généré les clés, vous pouvez utiliser la clé publique pour chiffrer les messages et la clé privée pour les déchiffrer.

Phase 2 : Chiffrement du message

Si **M** est un **entier** naturel strictement inférieur à n représentant un message, alors le message chiffré sera représenté par : $\boxed{C = M^{e} \bmod (n)}$ *(prenons Exemple : M=4 -> C=31)*

Phase 3 : Déchiffrement du message

$\boxed{M = C^{d} \bmod (n)}$

Exercise 01:

Alice souhaite envoyer le message "Hello" à Bob de manière sécurisée en utilisant RSA. Les paramètres de chiffrement sont les suivants : p = 17, q = 11, e=7

- Calculez N, l'entier de module RSA.
- Calculez $\phi(N)$, la fonction d'Euler de N.
- Vérifiez que e est premier avec $\phi(N)$.
- Trouvez l'exposant de déchiffrement d.

1. Bob choisit le mot "Hello" à envoyer à Alice. Utilisez le code ASCII pour transformer les lettres en chiffres entiers, puis utilisez la clé publique (N, e) pour chiffrer le message.
2. Alice utilise sa clé privée pour déchiffrer le message.

Série TD 04 : Signature électronique

Questions générales :

1. Sur quelle technique cryptographique est basée la signature numérique ? Expliquez ?
2. Est-ce que la technique cryptographique est appliquée directement sur le message ? Pourquoi ?
3. Quels objectifs de sécurité offre la signature numérique ?
4. Expliquer le principe de déroulement de la signature d'un document.
5. Que doit-on posséder pour signer un document électronique ? et pourquoi ?

Série TD 05 : Les Certificats Numériques

Exercice 1 : Voici deux cas pratiques

Cas 1 : Salma souhaite envoyer un courrier confidentiel à Mohamed, le scénario suivant va être exécuté:

- Elle va consulter un annuaire ou un serveur Web pour avoir la clé publique de Mohamed -
- Ensuite elle chiffrera le message en utilisant cette clé

Cas 2 : Mohamed envoie un document signé à Salma en utilisant sa clé privé (sans l'utilisation de certificat)

Questions :

1. 1. Quelle sont les risques de sécurité encourus dans les deux cas. Et comment y remédier ?
2. Qu'est-ce qu'un certificat électronique

Exercice 2 : Voici un exemple de certificat X509v3

1. Que représente chaque ligne de ce certificat ? La clé privée figure t'elle ?
2. Comment la signature de ce certificat est-elle calculée ?
3. Comment peut-on vérifier la validité de ce certificat ? Expliquer avec un schéma
4. Qu'est-ce qu'une autorité de certification ?

Certificate:

1. Data:
2. **Version:** 1.3
3. **Serial Number:** 234-A12
4. **Signature Algorithm:** md5withRSAEncryption
5. **Issuer:** C=ZA, SP=Western Cape, L=Cape Town, O=Thawte Consulting cc, OU=Certification Services, CN=www.thawte.com, Email=webmaster@thawte.com
6. **Validity**
7. Not Before: Nov 14 17:15:25 1999 GMT
8. Not After : Dec 14 17:15:25 2016 GMT
9. **Subject:** C=CH, SP=NE, L=Neuchâtel, O=Assoc. ABORD,
10. OU=Ermitage project, CN=projet-ermitage.org,
11. Email=admin@projet.ermitage.org
12. **Subject Public Key Info:**
13. **Public Key Algorithm:** rsaEncryption
14. **Modulus:**

00:9a:92:25:ed:a4:77:69:23:d4:53:05:2b:1f:3a:55:32:bb:27:de:0a:48
:d8:fc:c8:c0:c8:77:f6:5d:61:fd:1b:33:23:4f:f4:a8:2d:96:44:c9:5f:c
2:6e:45:6a:9a:21:a3:28:d3:27:a6:72:19:45:1e:9c:80:a5:94:ac:8a:67

15. **Exponent:** 65537 (0x10001)
16. **Signature Algorithm:** md5withRSAEncryption

7c:8e:7b:58:b9:0e:28:4c:90:ab:20:83:61:9e:ab:78:2b:a4:54:39:80:7b
:b9:d9:49:b2:b3:2a:fe:8a:52:f4:c2:89:0e:5c:7b:92:f8:cb:77:3f:56:2
2:9d:96:8b:b9:05:c4:18:01:bc:40: ee:bc:0e:fe:fc:f8:9b:9d:70:e3

TD 04

Signature électronique

Questions générales :

1. Sur quelle technique cryptographique est basée la signature numérique ? Expliquez ?

La signature électronique repose sur le principe de la cryptographie asymétrique.

Pour signer électroniquement un document le signataire utilise son certificat, qui constitue sa carte d'identité numérique. Ce certificat contient des informations sur son possesseur, ainsi que deux clés : une clé publique et une clé privée. La clé privée est utilisée pour signer le document, la clé publique est utilisée pour vérifier cette signature. Cela signifie que seul le possesseur du certificat (qui connait la clé privée) peut signer un document, mais que n'importe qui est en mesure de vérifier cette signature.

2. Est-ce que la technique cryptographique est appliquée directement sur le message ? Pourquoi ?

- Le condensat permet de vérifier l'intégrité des données
- On n'applique pas l'algorithme au message lui-même, mais à son condensat, obtenu à l'aide d'une fonction de hachage. La taille du condensat étant fixe et indépendante de la taille du message lui-même, cela permet de réduire la bande passante utilisée pour transmettre le message en plus la plupart des mécanismes de signatures numériques sont basé sur la cryptographie asymétrique. Cette dernière est coûteuse en calculs. L'appliquer sur des messages de taille arbitraire entraînerait une dégradation des performances du système

3. Quels objectifs de sécurité offre la signature numérique ?

- **Authentification** : Cela garantit l'identité de la personne qui a signé les données : l'origine du message, du document ou de la transaction est incontestable.
- **Intégrité des données** : La signature électronique protège l'intégrité des données. Cela signifie que le document reçu n'a pas été altéré, volontairement ou involontairement
- **non-répudiation** : L'auteur (la personne qui signe) d'un document prouve son identité. La non-répudiation établit, plus tard, qui a participé à une transaction. L'expéditeur ne peut nier avoir envoyé le message et le destinataire ne peut nier l'avoir reçu. Simplement, la non-répudiation signifie qu'une information ne peut être rejetée, tout comme avec les signatures manuscrites

4. Expliquer le principe de déroulement de la signature d'un document.

La signature d'un document se déroule comme suit :

a. Signature

Le signataire calcule le condensat du document à signer, puis il encrypte ce condensat à l'aide de sa clé privée. Il crée ensuite la signature, qui peut-être intégrée au document original ou enregistrée dans un fichier séparé. Cette signature est composée de l'empreinte signée (le condensat encrypté) et de son certificat.

b. Vérification

Le destinataire calcule le condensat du document reçu (en omettant la signature, si celle-ci est intégrée au document), et décrypte l'empreinte signée, à l'aide de la clé publique contenue dans le certificat du signataire. Il compare ces deux valeurs, si elles sont identiques, alors la signature est authentique, et l'identité du signataire est bien celle qui est décrite par le certificat. En vérifiant la validité de ce certificat, le destinataire est assuré de la validité de cette signature.

5. Que doit-on posséder pour signer un document électronique ? et pourquoi ?

On doit posséder un certificat numérique. Pour s'assurer que la clé publique que notre correspondant nous a communiqué est bien celle de la personne physique ou morale qu'il prétend être.

TD05

Certificats Numériques

Exercice 1 :

1. Il existe un risque d'usurpation d'identité :

Cas 1 : Dans le premier cas la confidentialité est compromise. Supposant, un pirate « Aissa » , a pu modifier l'annuaire ou le serveur Web qui contient la clé publique de « Salma ». Il a pu par exemple remplacer la clé publique de « Mohamed » par la sienne. Si « Salma », croit détenir la clé publique de « Mohamed » alors que c'est celle de « Aissa », elle envoie un message chiffré à « Mohamed » en le chiffrant avec la clé publique de « Mohamed ». Si celle-ci est en fait la clé publique de « Aissa », alors « Aissa » pourra déchiffrer ce message destiné à « Mohamed » avec sa clé privée. « Aissa » pourra donc lire le courrier confidentiel de « Mohamed ».

Cas 2 : « Aissa » pourra envoyer un message signé à « Salma » avec une signature générée avec sa clé privée et en se faisant passer pour « Mohamed ». « Salma » qui recevra le message vérifiera la signature du message avec ce qu'elle croit être la clé publique de « Mohamed ». La vérification sera correcte, donc « Salma » pensera que le message vient de « Mohamed ».

- Pour remédier à ce genre de problème on doit assurer la validité de la clé publique en utilisant le certificat numérique

2. Un certificat numérique : est un document électronique utilisé pour identifier un individu, un serveur, une entreprise ou toute autre entité et pour associer une clef publique à cette identité. Un certificat fournit généralement une preuve reconnue de l'identité de la personne. La cryptographie à clef publique utilise les certificats pour éviter les problèmes d'usurpation d'identité. Les certificats aident à prévenir l'utilisation de fausses clefs publiques.

Exercice 2 :

1. Chaque ligne représente :

Ligne 2 : version

Ligne 3 : Numéro de série unique, dans le domaine de confiance auquel appartient le certificat, qui l'identifie de façon unique. C'est ce numéro de série qui sera posté dans la liste de révocation en cas de révocation

Ligne 4 : Désigne le procédé utilisé par l'AC pour signer le certificat : (norme ISO). Il s'agit d'un algorithme asymétrique et d'une fonction de condensation.

Ligne 5 : Spécifie le DN (Distinguished Name) de l'AC qui a généré le certificat.

Ligne 6 : période de validité du certificat (les dates de début et de fin de validité du certificat).

Ligne 9 : Spécifie le DN de l'utilisateur possédant la partie privée de la clé publique contenue dans le certificat.

Ligne 12 : C'est le cœur du certificat. Ce champ contient la valeur de la clé publique du détenteur du certificat et les algorithmes avec lesquels elle doit être utilisée RSA with MD5 par exemple

Ligne 16 : Algorithme de signature + la Signature du certificat

2. Non la clé privée ne figure pas dans le certificat : Le certificat émis par l'AC lie une clef publique particulière au nom de l'entité qu'il identifie (tel qu'un nom d'employé ou de serveur). Seule la clef publique certifiée dans le certificat fonctionnera avec la clef privée correspondante possédée par l'entité identifiée par le certificat

3. Comment la signature de ce certificat est-elle calculée ?: Cette **signature électronique** est calculée sur les informations contenues dans le certificat comme dans le cas d'un message électronique. La signature est l'empreinte de ces informations chiffrée avec la clé privée de l'autorité de certification qui a délivré ce certificat.

4. Comment peut-on vérifier la validité de ce certificat ?: La validité du certificat peut être vérifiée en appliquant d'une part la fonction de hachage aux informations contenues dans le certificat, en déchiffrant d'autre part la signature de l'autorité de certification avec la clé publique de cette dernière et en comparant ces deux résultats. Evidemment, les dates de validité du certificat sont aussi vérifiées avant de le déclarer valide.

5. Une autorité de certification (AC) est un organisme reconnu comme étant compétent pour délivrer des certificats à une population auprès de laquelle elle a toute confiance et en assurer la validité. Elle s'engage sur l'identité d'une personne au travers du certificat électronique qu'elle lui remet. Une autorité de certification est responsable (vis-à-vis de ses clients, mais aussi de toute personne se fiant à un certificat électronique qu'elle a émis) de l'ensemble du processus de certification et, par voie de conséquence, de la validité des certificats qu'elle émet. Par ailleurs, c'est elle qui définit la politique de certification et la fait appliquer. Autant dire que son rôle et ses responsabilités sont importantes