SERIE DE TD N° 3

Exercice N°1 : Questions de cours :

1) Qu'est-ce qu'une PSSI ? Quels sont ses objectifs ?
2) Quelles sont les conditions de succès d'une PSSI ?
3) Quelles déférences entre les chartes et les bonnes pratiques ?
4) Qu'est-ce qu'un audit de sécurité ? et quelles sont ses pratiques ?
5) Citer les étapes de la gestion du contrôle d'accès.
6) A quoi sert de dépenser tant d'argents sur les recherches dans le domaine du chiffrement, alors qu'on est quasiment sûr que quel que soit l'algorithme de chiffrement adopté il arrivera bien le jour dans lequel celui-ci sera cassé ?
7) Quelle est la différence entre la sauvegarde et l'archivage ?
8) Qu'est-ce qu'un test d'intrusion ? et quelles sont ses 3 catégories ?
9) Quelles sont les avantages et les inconvénients du chiffrement symétrique et du chiffrement asymétrique ?
10) Pour chaque risque parmi les suivants, citer quelques mesures adéquates (donner des mesures de différents aspects) : vol de données sensibles situées dans un serveur connecté à internet, vol ou destruction d'un matériel important lors de son déplacement à la salle de maintenance, inondation au rez-de-chaussée.

Exercice N°2 :

Partie 1 : choisir les bonnes réponses (une ou plusieurs sont possibles)

1. **Instaurer à son personnel une habitude de travail nécessite une solution :**
   - ***A.*** *Purement technique.*
   - ***B.*** *Purement organisationnelle.*
   - ***C.*** *Purement juridique.*
   - ***D.*** *Technique/organisationnelle/juridique.*
   - ***E.*** *Technique/juridique.*
   - ***F.*** *Organisationnelle/juridique.*

2. **Installer une protection physique fait partie de la solution :**
   - ***A.*** *Purement technique.*
   - ***B.*** *Purement organisationnelle.*
   - ***C.*** *Purement juridique.*
   - ***D.*** *Technique/organisationnelle/juridique.*
   - ***E.*** *Technique/juridique.*
   - ***F.*** *Organisationnelle/juridique*

3. **Le scan de ports est une technique qui**
   - ***A.*** *Précède généralement les attaques informatiques.*
   - ***B.*** *Est considérée elle-même comme une attaque.*
   - ***C.*** *Est utilisée pour faire des audits de sécurité.*

4. **La stéganographie**

   A. *Est une technique de protection des réseaux.*

   B. *Appliquée en informatique ne peut contenir aucun risque.*

   C. *Peut-être combinée avec le chiffrement.*

   D. *Permet de garantir la confidentialité et l'intégrité de l'information.*

5. **Donner des exemples comment les faits suivants peuvent avoir une influence positive ou négative sur la sécurité du système :**

   A. *Procédures et méthodes de travail.*

   B. *Relation entre le personnel.*

   C. *Relation entre les employés et leurs supérieurs.*

   D. *Etats psychiques et sociaux du personnel.*

   E. *Absence/présence de pénalité/récompense.*

Partie2 : Répondre aux questions suivantes :

1. Comment la PSSI améliore le rôle du RSSI?
2. Pourquoi l'entreprise a-t-elle besoin de définir son propre règlement intérieur, malgré l'existence des Lois du pays?
3. Sécuriser son système consomme généralement beaucoup d'argent sans aucun gain monétaire évident ; y a-t-il pas de solution alternative ? Discuter son efficacité.
4. Comparer le processus de chiffrement symétrique vs celui du chiffrement asymétrique.
5. Comparer le processus de cryptographie vs celui de la stéganographie.
6. S'il y a dans un système N utilisateurs qui partagent des secrets deux à deux :
   - Combien de clés doit en disposer chacun d'eux s'ils utilisent un chiffre symétrique ? asymétrique ?
   - Combien de clés doit y en avoir dans ce système dans les deux cas ?
7. Les mécanismes utilisés pour faire des audits de sécurité.
8. Mécanismes de protection physique ?
9. Mécanismes de protection logique ?
10. Pourquoi et comment communiquer son PSSI ?

Partie 3 : Rechercher sur Internet :

1. **Termes :**

Cybersquattage;	*Attaque MITM ;*	*Attaques XSS ;*
Phishing ;	*Wardriving ;*	*Cartographie du réseau ;*
Ingénierie sociale ;	*Canulars informatiques;*	*Attaque force brute ;*
DoS, DDoS ;	*Scam ; Spam ;*	*Attaque par dictionnaire ;*
Manipulation d'url ;	*IP Spoofing ;*	*Keylogger ; Snifer ;*
ARP Poisoning ;	*Smurfing ;*	*DND Poisonning ;*
TCP Session Hijacking;	*SYN Flooding ;*	*Cracker, Hacker.*

2. Comment la commande « ping » est utilisée dans les attaques.
3. Comment tracer un mail ?
4. Comment choisir un bon mot de passe ?
5. Authentification OTP : définition et principe.
6. Expliquer les mécanismes de sauvegarde, d'archivage, et de contrôle d'accès ; les moyens utilisés, leurs avantages / inconvénients.
7. Donner la définition, le rôle , le principe de fonctionnement, les avantages/inconvénients des outils :

– Firewall.	– Proxy.	– VPN.
– IDS, NIDS.	– Antivirus.	– Nessus, Nmap
– IPS, HIPS.	– DMZ.	– Wireshark ;

8. Comment mener une investigation numérique ?

Exercice N° 3 :

Discuter l'efficacité des idées suivantes :

a. *Utiliser les logiciels de scan de port sur les machines de son réseau ?*
b. *Utiliser les logiciels de contrôle à distance ?*
c. *Répartir les données sensibles sur plusieurs postes ?*
d. *Se connecter à internet derrière une machine proxy ?*
e. *Ne jamais répondre ni à un Spam ni à un canular (hoax) ?*
f. *Utiliser plusieurs antivirus sur le même réseau ?*
g. *Se connecter à internet à travers une session administrateur ?*
h. *Utiliser le même mot de passe partout ?*
i. *Faire des audits de sécurité régulièrement ?*
j. *Donner aux utilisateurs ayant un accès limité la possibilité de changement de la séquence de démarrage du système d'exploitation ?*

k. *Autoriser l'utilisation des freewares et des sharewares ?*

l. *Utiliser plusieurs antivirus sur le même poste ?*

m. *Fouiller le personnel à chaque entrée ou sortie de l'entreprise ?*

n. *Garder la trace de chaque accès aux ressources sensibles ?*

o. *Donner aux utilisateurs ayant un accès limité le droit de lecture/écriture et modification de leurs propres données ?*

p. *Attribuer à chaque utilisateur une paire (login/mot de passe) unique et différente de celles des autres ?*

Exercice 4 :

Soient les 3 chiffres expliqués ci-dessous :

Chiffre Atbash : consiste à inverser l'ordre des lettres de l'alphabet :

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

Chiffre Albam : qui décale les lettres de 13 positions :

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

Chiffre Atbah :

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

1) A quel type de chiffre appartiennent ces algorithmes ? Sont-ils réversibles ?
2) Quelles sont les clés de chiffrement pour chacun ?
3) Respectent-ils le principe de Kerckhoffs ?
4) Comparer ces algorithmes avec celui du César qui consiste à appliquer un décalage d sur les lettres de l'alphabet.

Exercice 5 :

Calculer les clés publiques et les clés privées pour les utilisateurs qui ont choisis d'utiliser l'algorithme RSA avec les paramètres p et q suivants :

- p = 211, q =109
- p = 113, q = 81
- p = 5, q = 7
- p = 1013, q = 397
- p = 615, q = 23

Chiffrer le proverbe chinois suivant pour les cas précédents :

M = "QUAND LE SAGE MONTRE LA LUNE LABRUTI REGARDE LE DOIGT"

Exercice 6 :

Soit un système qui utilise un chiffre à clé publique; ce système contient 3 utilisateurs A, B et C qui ont respectivement les paires de clés suivantes (K_A, K'_A), (K_B, K'_B), (K_C, K'_C) sachant que la 1ère clé de chaque paire est la clé publique et la 2ème est la clé privée.

a) Pour chaque fait parmi les suivants expliquer comment l'émetteur et le destinataire doivent procéder ? (préciser les clés utilisées et leur ordre d'utilisation).

1. A envoie un message secret à B. (1pt)

2. C diffuse un message chiffré contenant la mise-à-jour des clés publiques de tous les utilisateurs. (1pt)
3. B envoie un message secret et signé à A. (1pt)
4. A envoie un message secret avec condensat signé à B. (1pt)

NB : on peut utiliser la notation mathématique : (E : chiffrement, D : déchiffrement, M message en clair, C message chiffré et H fonction de hachage)

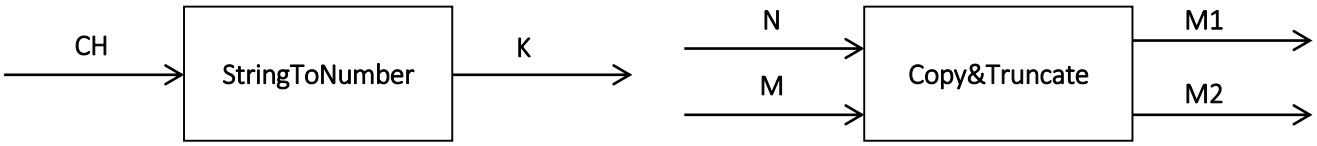
b) Quels sont les objectifs satisfaits pour chaque fait ? (1pt)

Supposons que les clés publiques sont sauvegardées en clair dans un annuaire accessible par tout utilisateur. Si un attaquant P arrive à pénétrer dans ce système et veut jouer le rôle du « man in the middle » entre A et B en falsifiant leurs clés.

c) Expliquer comment doit-il procéder ? Peut-il arriver à ses fins ? (1pt)

Exercice N°7 : (7pts) : (EMD 18-19)

On dispose de deux procédures suivantes :



La procédure **StringToNumber(CH,K)** prend en entrée une chaine de caractères CH et fournit en sortie un vecteur K d'entiers, tel que chaque caractère C_i dans CH est remplacé dans le tableau K par son ordre dans l'alphabet par rapport aux autres caractères dans la chaine CH. Si le même caractère apparait plusieurs fois, ces occurrences auront des ordres successifs en commençant par la première occurrence à gauche. (Voir l'exemple 1 dans l'annexe).

La procédure **Copy&Truncate(M,N,M_1,M_2)** prend en entrée une chaine de caractère M et un entier positif N, et fournit en sortie deux chaines de caractères M_1 et M_2, tels que :

M_1 contient les N premiers caractères de M, et M_2 contient le reste des caractères de M. Si N est supérieur ou égale au nombre de caractères dans M, M_1 sera égale à M et M_2 sera vide. (Voir l'exemple 2 dans l'annexe).

Soit la fonction de chiffrement ***Chiffre*** décrite dans l'annexe.

a) Calculer les messages C_1 = Chiffre(M,K_1) et C_2 = Chiffre(M,K_2) pour **(2pts)** :
- **M = *'LA COMPLEXITE EST LE PIRE ENNEMI DE LA SECURITE'*** ;
- **K_1 = *'EXAMEN'*** ;
- **K_2 = *'UNIVERSITE'*** ;

b) A quelle classe de cryptographie appartient ce chiffre ? **(0.5pts)**

c) Respecte-t-il le principe de KERKCHOFF ? **(0.5pts)**

d) Discuter la sensibilité de ce chiffre à l'attaque statistique et à l'attaque à texte clair. **(1.5pts)**

On peut remarquer que pour chaque clé K on peut trouver une très longue liste de mots (ayant un sens ou non) qui donnent le même résultat de chiffrement. Appelant ces mots 'Clés Analogues'.
- Par exemple les mots suivants sont des clés analogues à la clé K='ALGER' :
- 'ALIAS', 'ANGES', 'ARMER', 'CLICS', 'COLIS', 'CRIER', 'DROIT', 'ADCBE', 'BDCBF', …

e) Trouver deux clés analogues à K_1 et à K_2 (ayant un sens ou non). **(0.5pts)**

On peut vérifier que lorsqu'on chiffre un message avec la clé K_1 ou une de ses clés analogues, on peut déchiffrer le message résultat avec la clé K'_1 ='MARQUE' ou une de ses clés analogues suivantes :

- 'CAEDFB', 'FAMINE', 'GAMINE', 'FEIGNE', 'MASQUE', 'NATRUM', 'SCUTUM', …

f) Proposer une clé de déchiffrement pour K_2. **(0.5pts)**

Donner une méthode (algorithme) pour trouver une clé de déchiffrement K' à partir de celle de chiffrement K. **(1.5pts)**

Annexe :

Exemple1 :

StringToNumber	CH = TOUT	K = [2 , 1 , 4 , 3]
	CH = ELEGANCE	K = [3 , 7 , 4 , 6 , 1 , 8 , 2 , 5]

Exemple2 :

Copy&Truncate	M = UNIVERSITE , N = 5	M_1 = UNIVE, M_2 = RSITE
	M = JIJEL , N = 7	M_1 = JIJEL , M_2 = Ø

Fonction de chiffrement :

```
Fonction Chiffre( M, K :chaine de caractères) : chaine de caractères
 Var M1, C, C1 : chaine de caractères
 Key : tableau d'entiers
 i, j : entiers
Début
  StringToNumber(K,Key)
  M←MessageSansEspace(M)     // cette fonction enlève tout espace entre les caractères.
  C ←Ø
  Tant que (M ≠ Ø) ET (Longueur(M) ≥ Longueur(K)) Faire
     C1 ←Ø
     Copy&Truncate(M, Longueur(K), M1, M)
     Pour i ← 1 à Longueur(K) Faire
        C1 ←C1 + M1[Key[i]]
     Fin Pour
     C ← C + C1
  Fin Tant que
  Si Longueur(M)> 0 Alors
     C ←C + M
  Fin Si
  Retourner(C)
Fin.
```