

1 Exercice (8 points)

Le service de sécurité qui sera atteint dans les cas de figures suivants :

- Un attaquant a réussi à consulter un fichier transitant sur le réseau. Il arrive à voir son contenu mais il n'arrive pas à le décrypter.... **Aucun service** **Le pirate n'arrive pas à consulter l'information**
- La base de données d'aire Algérie a été attaquée et toutes les places disponibles sur le vol Londres ont été réservées au nom de "L3 ISIL".**L'intégrité** **La donnée a été modifier avec une personne n'ayant pas ce droit**
- Un pirate utilise une adresse IP volée pour convaincre un système qu'il est un client fiable et connu.**Le contrôle d'accès** **Une personne fait passer et avoir les droits de quelqu'un d'autre dans un système qu'il a ccès**
- Un attaquant a réussi à consulter un fichier transitant sur le réseau. Il arrive à voir son contenu et arrive à le décrypter et le lire.**La confidentialité** **La donnée est consulté avec une personne qui n'a pas ce droit**
- Un utilisateur supprime accidentellement un fichier et pour ne pas être sanctionné il cache cet acte.**La non-répudiation** **Un utilisateur arrive à niée un acte qu'il a commit effectivement**
- Un pirate bombarde un serveur de BD par des requêtes sans arrêt.**La disponibilité** **Cet acte peut rendre le serveur indisponible pour les utilisateurs légitimes dans les périodes de service**
- Un pirate réussi à utiliser la carte bancaire d'un individu et se fait payer un iPhone sur le site d'Apple.**L'authentification** **Une personne fait passer et avoir les droits de quelqu'un d'autre**
- Les pirates injectent du contenu dans une page qui corrompt le navigateur de la cible. Il peut ainsi modifier la page web selon ses envies.**L'intégrité** **Une personne non autorisée à réussi de modifier la donnée**

2 Exercice (8 points)

1. CRYPTÉ :ZKVKCDSXO GSVV LO PBOO FOBI CYYX

La fréquence :Z=1,K=2, V=3,C=2, D=1, S=2,X=2,O=5, G=1, L=1, P=1, B=2, F=1, I=1, Y=2(2 Pts)

La lettre la plus fréquent est le **O** alors, La clé : **K=10**(2 Pts)

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

Claire : **PALASTINE WILL BE FREE VERY SOON**(2 Pts)

2.Claire : "la rencontre est prévue à l'université"

Crypté : **BX CHSYFSMCH HVM LCHEU X LUSZEHCVZMH** (2 pts)

3 Exercice (4 points)

- Alice veut envoyer un message chiffré à Bob (Bob sera le seul capable de lire le message), avec quelle clef doit-elle le chiffrer ? **PK_{Bob}** . A l'arrivée, quelle clef, Bob doit-il utiliser pour déchiffrer le message ? **SK_{Bob}**
- Alice veut envoyer un message signé à Bob, avec quelle clef doit-elle le signer ? **SK_{Alice}** . A l'arrivée, quelle clef, Bob doit-il utiliser pour vérifier la signature du message ? **PK_{Alice}**
- Alice veut envoyer un message signé et chiffré à Bob, avec quelle clef doit-elle le signer ? **SK_{Alice}** . Le chiffrer ? **PK_{Bob}** . A l'arrivée, quelle clef, Bob doit-il utiliser pour : Déchiffrer le message ? **SK_{Bob}** . Vérifier la signature ? **PK_{Alice}** .