FSBM
2024-2025
Master DSBD
Sécurité de données & Blockchain

TD1- Introduction à la sécurité de données

Exercice 1

I. Questions

1. Qu'est-ce qu'un malware ?
2. Quelle est la différence entre un virus et un ver informatique ?
3. Donnez trois types de malwares et expliquez leur fonctionnement.
4. Quelles sont les principales méthodes de propagation d'un malware ?
5. Quel est le rôle d'un cheval de Troie (Trojan) ?

II. Un employé d'une entreprise reçoit un email lui demandant de réinitialiser son mot de passe via un lien. Il clique dessus et entre ses identifiants. Peu de temps après, son compte est utilisé pour envoyer des emails suspects.

1. Quel type d'attaque a eu lieu ?
2. Quels signes auraient pu alerter l'employé ?
3. Quelles mesures de protection auraient pu éviter cette attaque ?
4. Identifiez les objectifs fondamentaux (services) en sécurité informatique. Puis, expliquez la différence entre eux.

Exercice 2 : Attaque par force brute

Un message a été chiffré avec le chiffrement de César, mais la clé est inconnue. Le message chiffré est :
"ZHOFRPH WR WKH ZRUOG RI FUBSWRJUDSKB"

1. Décryptez le message en essayant toutes les clés possibles.
2. Quelle est la clé correcte ?
3. Écrivez un programme qui automatise cette attaque.

Exercice 3 : Analyse fréquentielle

Un attaquant intercepte le message chiffré suivant :
"YMNX NX F YMJWXJYJ"
Sachant que le chiffrement de César conserve la fréquence des lettres, utilisez une analyse fréquentielle pour retrouver la clé et déchiffrer le message.

Exercice 4 : Chiffrement et déchiffrement

I. Une substitution monoalphabétique utilise une permutation aléatoire de l'alphabet. On vous donne la clé suivante :

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

1. Chiffrez le message : **"INFORMATION SECURITY"**.

2. Déchiffrez le message chiffré suivant avec la clé ci-dessus :
   "UEOTGQGQITG KTGIKFGZO"
3. Proposez une méthode d'attaque contre ce chiffrement.

II. On utilise la clé **"CRYPTO"** pour chiffrer un message avec Vigenère.

1. Chiffrez le message **"SECURITY SYSTEM"**.
2. Déchiffrez le texte chiffré suivant avec la clé **"KEY"** :
   "RIJVS UYVJN".

Exercice 5

Considérons le message *M* = LATECHNOLOGIEBLOCKCHAIN.

1. Soit *K* = ULOIDTGKXYCRHBPMZJQVWNFSAE une clé de substitution.
   a. Trouver le chiffrement de *M*.
   b. Quelles propriétés du texte clair et du texte chiffré restent inchangées par un chiffrement à substitution ?
2. Chiffrement par transposition
   a. Trouver le chiffrement de M par transposition avec la clé [3,5,2,6,1,4].
   b. Quelles propriétés du texte clair et du texte chiffré restent inchangées par un chiffrement à substitution ?
3. Chiffrement de Vigenère
   a. Trouver le chiffrement de *M* par un chiffrement de Vigenère avec la clé SECURITE.
   b. Qu'est-ce se passe aux fréquences des caractères dans un texte chiffré avec un chiffrement de Vigenère ?