Semestre 1 Licence 3 Ingénierie Informatique: Option R&S Cours Sécurité des Réseaux

TD1 : Cryptographie

Chiffrement traditionnel

Soit le tableau de correspondance suivant entre l'alphabet et les entiers.

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.

0 - 1 - 2 3 - 4 - 5 - 6 - 7 - 8 -9 -10 -11-12-13 -14- 15- 16 -17-18-19 -20- 21- 22-23- 24-25.

Soit le message M = WELCOMETOUASZ.

Exercice 1 :

1. Trouver le chiffrement C de M en utilisant la méthode de César avec une clé K=5 ?
2. Pour une lettre X du message M, donner une formule mathématique F permettant de trouver l'entier correspondant à la lettre qui doit la remplacer dans le cryptogramme C ?
3. Si on connait la clé K, quel est le nombre de fois qu'on doit appliquer la formule mathématique F pour chiffrer M ?
4. Si la clé K n'est pas connu, quel est le nombre de fois maximum N et le nombre de fois minimum n qu'on appliquer la formule mathématique F pour trouver C ?
5. N et n sont-ils fonction de la longueur de M ?
6. A l'aide d'un formule mathématique ou algorithme, trouver la formule de déchiffrement de C ?

Exercice 2 :

Soit K une clé de substitution d'un chiffrement mono-alphabétique, K est obtenu par tirage successif sans remise des 26 lettres alphabétiques

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

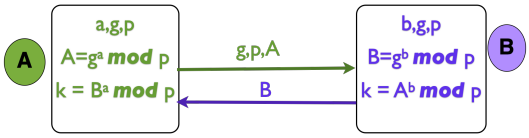
K =. P O I U Y T R E Z A Q S D F G H J K L M W X C V B N

1. Trouver C le chiffrement de M: C = E(K, M) ?
2. Si la clé K n'est pas connu, quel est le nombre maximum de clés N et le nombre minimum de clés n à utiliser pour trouver C ?
3. Quelle sera la longueur de la clé pour chiffrer des chiffres et lettres ? Et dans ce cas, quel sera le nombre maximum de clés à utiliser pour trouver un cryptogramme ?
4. Trouver la clé inverse K^{-1} de déchiffrement de C ?// B prend la position de Y donc dans la clé inverse, Y sera à la position de B ($2^{ème}$)
5. Chiffrer le message M par transposition en utilisant la clé K=[1-6-4-2-3-5]:C=E(K, M) .
6. Déterminer la clé K^{-1} associée à la clé de transposition K, puis retrouver M à partir C ?
7. Si on ne connait que la longueur ou taille de la clé, quel sera le nombre maximum de clés à utiliser pour trouver un cryptogramme de même taille que la clé ?
8. En utilisant le chiffrement de Vigenère, chiffrer M avec la clé K = MASTER.
9. Trouver la clé K^{-1} associée à la clé de Vigenère MASTER ?

Protocole d'échange

Exercice 3 : échange de clé

La cryptographie à clé symétrique est économe en ressource (cpu, mémoire etc..) car ses clés sont courtes et permettent de chiffrer/déchiffrer très rapidement. Cependant il existe un problème de partage de la clé au moins entre deux entités communicantes. Dans cette exercice, la méthode Diffie-Hellman est étudiée pour partager une clé symétrique.



1. Trouer le clé symétrique partagée après l'échange ?
2. Quelles sont les valeurs secrètes (confidentielles) contenues dans cette clés ?
3. Si $g=5$ et $p= 13$, calculer la clé partagée si A et B ont choisi d'utiliser respectivement $a=3$ et $b= 5$?
4. **Attaque sur la confidentialité de la clé**: par force brute, on peut tenter de trouver la clé une fois qu'on a accès aux 2 messages échangés. Il suffira de trouver ces valeurs secrètes. Pour se faire, il faudra alors résoudre un problème difficile. Étant donné g, p et A, il est très difficile de connaitre à tel que $A= g^a \bmod p$: a est le logarithme discret de A dans la base g, c'est le ***problème Logarithme discret***.

   Pour un Hacker H, quel est le nombre de multiplications à calculer pour obtenir la clé par force brute si a et b sont choisis dans l'intervalle [1, 5]?
5. **Attaque sur l'authentification**: Si g et p sont suffisamment grand et bien choisis, il sera très difficile pour H de trouver la clé. Ainsi il peut tenter compromettre l'authentification. Trouver le modèle du Hacker H pour se faire passer de A auprès de B ?
6. Trouver le modèle du Hacker H pour se faire passer de A auprès de B et de B auprès de A?

Exercice 4 : échange de message

A veut envoyer un message $M \in \{0,1\}^n$ à B. A possède une clé secrète a et B possède une clé secrète b de même longueur que M. Ils effectuent le protocole suivant :

1- A envoie $A_1 = M \oplus a$ à B

2- B envoie $B_1 = A_1 \oplus b$ à A

3- A envoie $A_2 = B_1 \oplus a$ à B.

Montrer que B peut retrouver le message M. Montrer que si C a intercepté tous les échanges, il peut également retrouver M.