TD2

Mécanismes cryptographique de la sécurité

Exercice 1 :

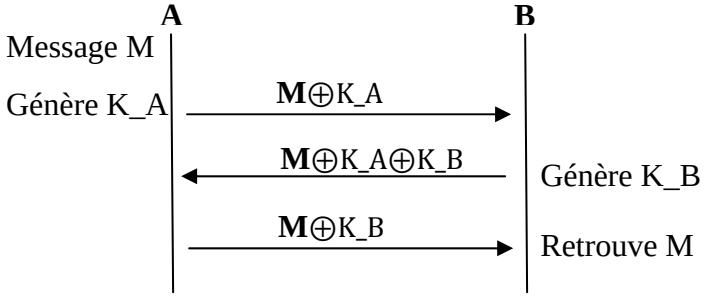
Soit un système de communication à N nœuds où les messages échangés entre les nœuds peuvent être facilement écoutés. Quel est le nombre de clés à maintenir par chaque nœud pour assurer une communication secrète entre chaque paire de nœuds :

a. Pour un système à clés symétrique ? ➔n-1 clés
b. Pour un système à clé asymétrique ? ➔2 clés (pulique, privée)

Exercice 2 :

Soit **M** un message et **K** une clé aussi longue que **K**. On note **C**=**M**⊕**K** le message **M chiffré avec K.** Si m[i] est le i^{ème} bit du message m et k[i] est le i^{ème} bit de la clé K, alors le i^{ème} bit de M⊕K est égal à (M[i] ⊕ K[i]))

1) Montrez que le "ou exclusif ⊕ " est une technique de chiffrement symétrique. ➔ on chiffre et on déchiffre avec la même clé. **C**=**M**⊕**K** ➔ **C**⊕K=**M**⊕**K**⊕K=M
2) Est-il pratique de stocker des clés symétriques aussi longues que les messages à chiffrer? ➔ c'est non pratique vu qu'il faut changer la clé à chaque fois que le message change de taille
3) Soit le protocole suivant qui exploite le "ou exclusif ⊕ " pour le chiffrement d'un message M. Quand A veut envoyer un message M à B, il génère une clé K_A aussi longue que M. B génère aussi une clé K_B aussi longue que M.
    c. Comment B peut-il déterminer la taille de la clé K_B ? ➔ c'est la même taille de **M⊕K_A**
    d. Comment A peut-il déterminer M⊕K_B à partir de M⊕K_A⊕K_B ? ➔il ajoute sa clé : M⊕K_A⊕K_B ⊕**K_A=** M⊕K_B
    e. Comment B retrouve t-il M ? ➔ il ajoute sa clé : M⊕K_B⊕K_B=M
    f. Si tous les messages échangés peuvent être écoutés, ce protocole permet-il la confidentialité. ➔ non : un ⊕ entre les trois message donne M



Rappel : $A \oplus A = 0$; $A \oplus 0 = A$;

Exercice 3 :

Soit l'échange de messages suivant entre 3 entités A, B et C (un intrus) utilisant un système de chiffrement asymétrique. Nous utilisons le format suivant (source, destination, message)

1) Quel est le traitement **Trt** effectué par C. ➔ déchiffrement avec sa clé privée et chiffrement avec la clé publique de B
2) A et B se rendent-ils compte de l'existence de l'intrus C ➔ non
3) Proposer une solution permettant de remédier à cette attaque ➔ authentification forte : certificat