UMBB, Faculté des Sciences Département d'Informatique		L3 Matière : Sécurité Informatique

Test Sécurité Informatique 2021-2022

Exercice 1:

1- Quelles sont les deux problèmes que le cryptage hybride permet de résoudre.
2- Expliquer le rôle d'une clé publique et une clé privée dans les signatures numériques.
3- Pourquoi les Certificats de Sécurité sont générés par une entité indépendante?

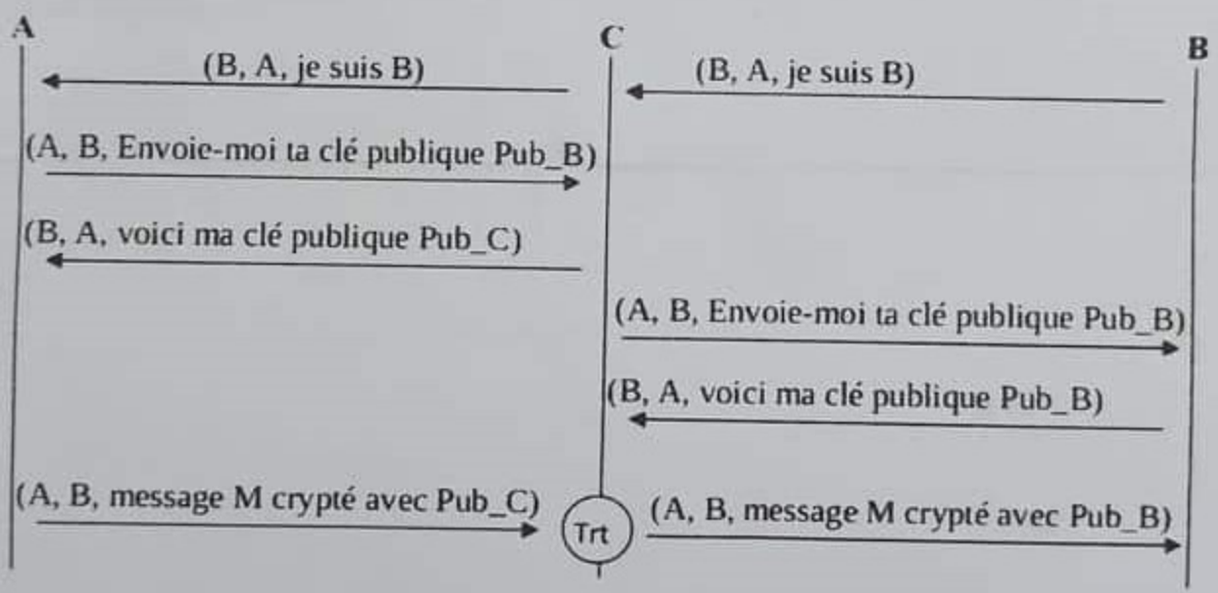
Exercice 2:

Déchiffrez le message '**cuskqxwmfwituk**' crypté avec Vigenère utilisant la clé suivante :

'**quauwtedbdisjg**' (a=0, b=1, etc..). Qu'avez-vous remarqué ?

Exercice 3:

La figure 1 présente l'échange de messages entre 3 entités A, B et C (un intrus) utilisant un système de chiffrement asymétrique. Nous utilisons le format des messages suivant: (source, destination, « message »).



1) Quel est le traitement **Trt** effectué par C ?
2) A et B se rendent-ils compte de l'existence de l'intrus C? De quelle attaque s'agit-il?
3) Proposer une solution permettant de remédier à cette attaque