Exercice 1 :

Un groupe de n étudiants souhaite utiliser un système cryptographique pour s'échanger deux à deux des informations confidentielles. Les informations échangées entre deux membres ne doivent pas être lues par un autre membre.
Le groupe décide d'utiliser un système de chiffrement Symétrique.

1. Quel est le nombre minimal de clés Symétriques nécessaires ?
2. Donner un nom d'un système Symétrique (algorithme) connu.

Le groupe décide après d'utiliser un Système de chiffrement Asymétrique.

3. Quel est le nombre minimal de couples de clés Asymétriques nécessaires pour que chaque membre puisse envoyer et recevoir des informations chiffrées ?
4. Ahmed souhaite envoyer des informations chiffrées et signées à Ali (Ahmed et Ali appartiennent tous les deux au groupe). Quelle(s) clef(s) Ahmed doit-il utiliser ?
5. Donner le nom d'un algorithme de chiffrement asymétrique reconnu.

Le groupe décide finalement d'utiliser un système hybride pour le chiffrement (combinaison entre systèmes Symétrique et Asymétrique).

6.Donner les raisons qui ont poussées ce groupe à utiliser un tel système

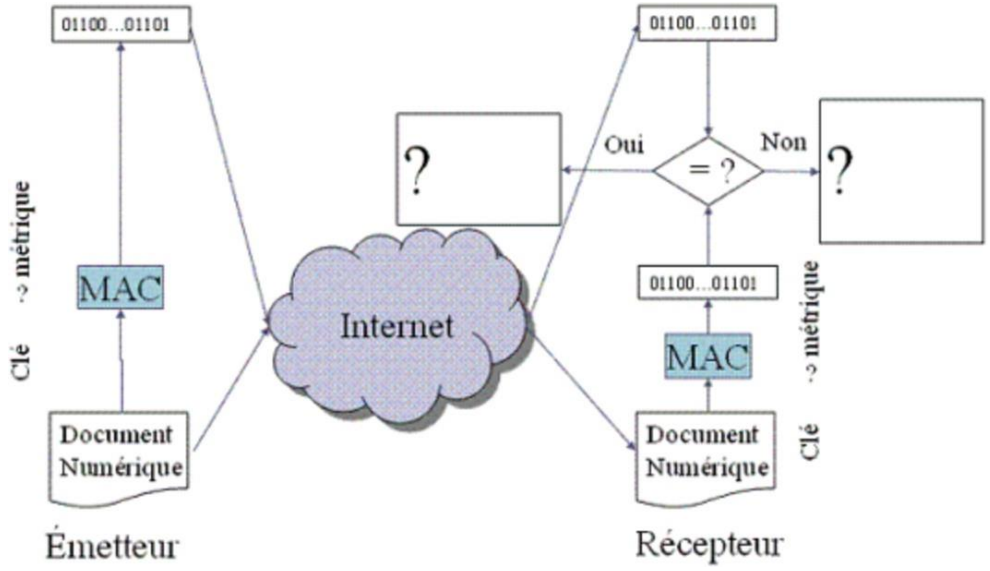
Exercice 2 :

Nadia, qui utilise souvent la messagerie sécurisée de son entreprise, vient de perdre sa clé privée, mais dispose encore de la clé publique correspondante.

1. Peut-elle encore envoyer des courriers électroniques chiffrés ? En recevoir ?
2. Peut-elle encore signer les courriers électroniques qu'elle envoie ? Vérifier les signatures des courriers électroniques qu'elle reçoit ?
3. Que doit-elle faire pour être de nouveau capable d'effectuer toutes les opérations mentionnées ci-dessus ?

Exercice 3 : QCM

Ce schéma



- ☐ Assure l'authentification de l'origine
- ☐ Utilise une clé asymétrique
- ☐ Permet d'assurer l'intégrité du Document Numérique échangé
- ☐ Utilise un MAC qui est une fonction de hashage paramétrée par une clé
- ☐ Permet de signer le document pour assurer la non répudiation