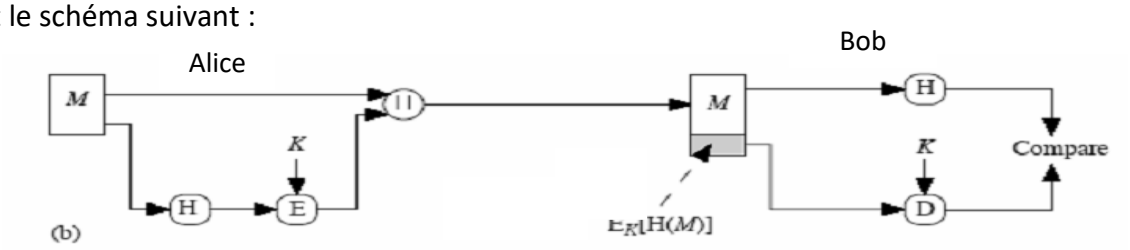
Exercice N° 01:

Soit le schéma suivant :



1. Ecrire formellement le message émis
2. Expliquer brièvement le processus exécuté par Bob
3. Quelles sont propriétés validés par ce protocole?
4. Quelles sont les primitives utilisées par Bob?
5. Quel est le type de la fonction de hachage utilisée?

Exercice N° 02:

1. Décrire le schéma de génération de clés, schéma de signature, et schéma de vérification.
2. Quelles sont les propriétés de sécurité validées par ce schéma ?
3. Soient p=11 et q=23, calculer N et $\Phi(n)$.
4. Si la clé de vérification égal à 7, calculer la clé de la signature.
5. Calculer la signature de h(m) = 10 ?

Exercice N° 03:

Ci-après 8 définitions des programmes malveillants et à vous d'attribuer à chacun le nom du programme malveillant correspondant :

1. Fragment qui se propage à l'aide d'autres programmes.
2. Programme autonome, Proches des virus mais capables de se propager sur d'autres ordinateurs à travers le réseau.
3. Programme utile qui contient un programme malveillant.
4. Accès caché à un ordinateur.
5. Programme qui envoie tes informations personnelles à d'autres.
6. Programme est chargé d'enregistrer à son insu ses frappes clavier pour intercepter des informations sensibles, comme les mots de passe.
7. Programme à la capacité de verrouiller l'écran d'un ordinateur ou de chiffrer des fichiers importants.

Les noms à attribuer : Keylogger, cheval de Troie, Virus, Ver, Ransomware, spyware, Backdoor