Université d'Alger1
Faculté des sciences
Département informatique
Module : Sécurité des systèmes d'information Licence ISIL - 2021/2022

Série TD *3*

Fonctions de Hachage et signatures numériques

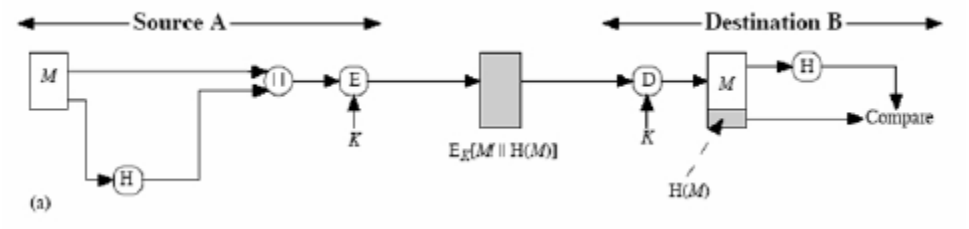
Exercice 1 :

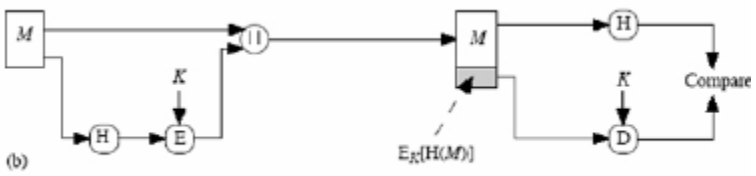
Soit M un message clair, E un algorithme de chiffrement symétrique, k une clé secrète partagée entre Alice et Bob, H une fonction de hachage et || l'opération de concaténation. Quels sont les objectifs de sécurité assurés dans chacun des scénarios suivants :

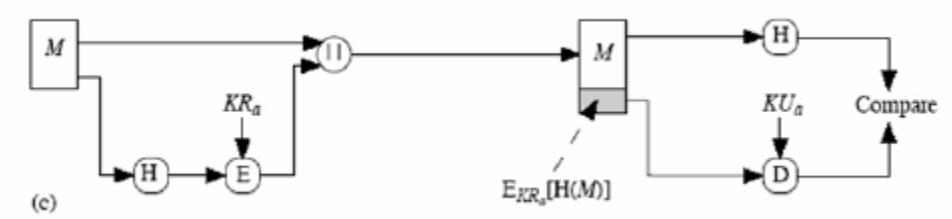
1) *Alice envoie à Bob : $M \| H(M)$.*
2) *Alice envoie à Bob : $E_k(M)$.*
3) *Alice envoie à Bob : $E_k(M) \| H(M)$.*

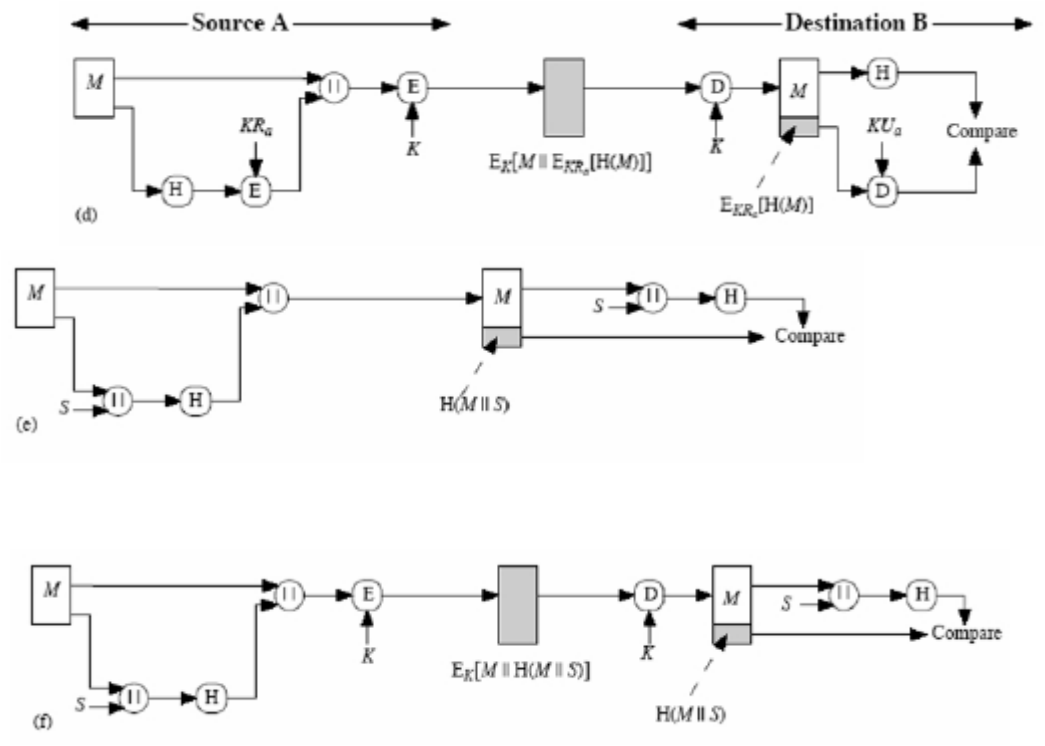
Exercice 2 :

Soient les exemples d'utilisation de la fonction de hachage ci-dessous. Expliquez les objectifs de sécurité visés dans ces exemples (entre la confidentialité, l'intégrité, l'authentification et le non répudiation).
(KU : la clé publique, KR : la clé secrète)









Exercice 3 : Signature El-Gamal (DSS)

Soit la clé privé a =8, p=11 et g=2.

1. Trouver la clé publique
2. Calculer la signature du message M=5
3. Vérifier la validité de la signature

Exercice 4 : Signature RSA

1. Calculer N et φ (n) associés aux nombres p=17 et q=23.
2. Quels sont les exposants secrets de signatures associées aux exposants publics e=11 et e=13 ?
3. Quelle est la signature de m=100 ?
4. Vérifier que la signature fonctionne.