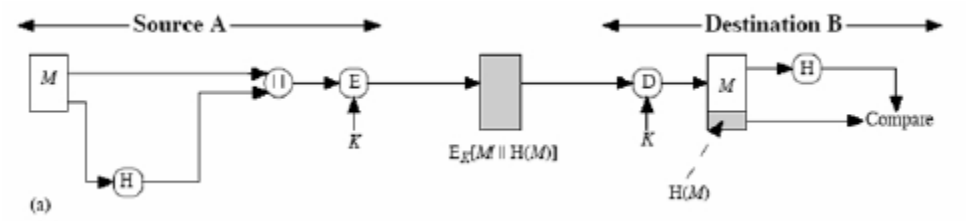
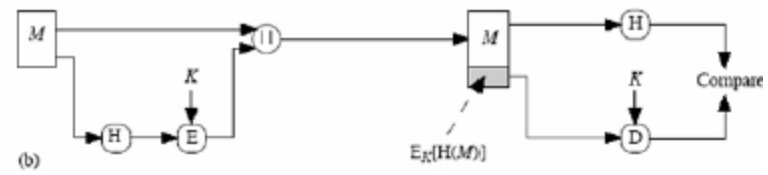
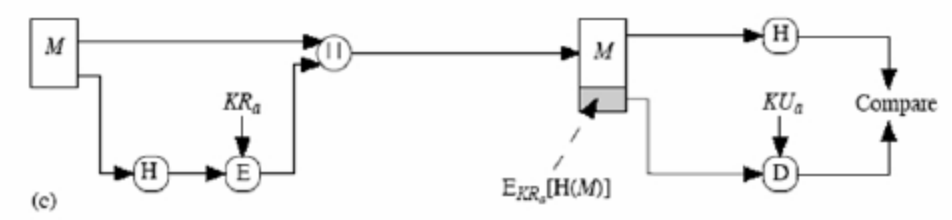
Exemple de l'utilisation de la fonction de hachage



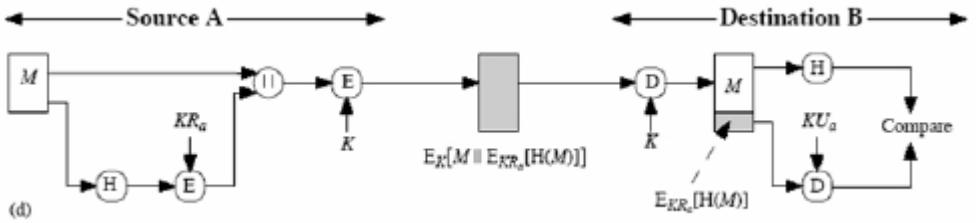
Principe : Le message concaténé à un hash code est chiffré en utilisant le chiffrement symétrique**.**
Confidentialité par le chiffrement symétrique du message et du code de hachage
Intégrité : par le bloc haché
Authentification : par l'utilisation de la clé secrète => Puisque seuls A et B partagent la clef secrète, le message doit provenir de A et n'a pas été modifié



Principe : seul le haché est chiffré, en utilisant le chiffrement symétrique ; Ceci réduit le traitement pour les applications qui n'exigent pas la confidentialité
Intégrité : par le bloc haché
Authentification : par l'utilisation de la clé secrète
Car le bloc authentificateur ne se base plus uniquement sur le message, mais également sur une clé secrète. On parle de la fonction MAC (fonction de hachage + clé secrète).

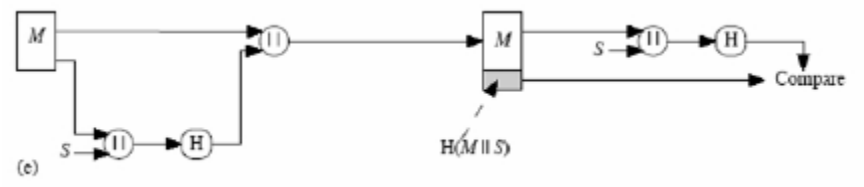


Principe : Le code de hachage est chiffré, en utilisant le chiffrement par clef publique et la clef privée de l'expéditeur
Intégrité : par le bloc haché
Authentification : par l'utilisation de la clé secrète de l'expéditeur
Non-répudiation : par l'utilisation de la clé secrète de l'expéditeur qui est une information unique propre à l'expéditeur pour empêcher le démenti (le récepteur utilise la clé publique)
C'est le principe de Signature numérique car seul l'expéditeur pourrait avoir produit le code de hachage chiffré.

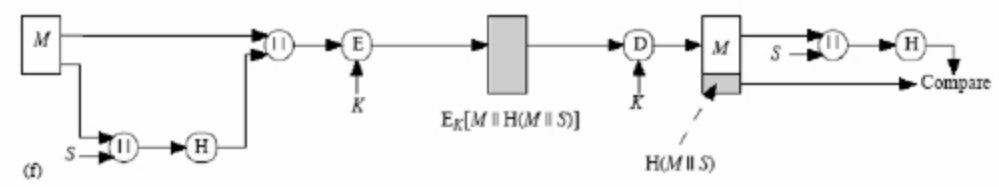


Principe : Le message et le code de hachage chiffré avec la clé privée sont chiffrés en utilisant une clef secrète symétrique.
Confidentialité par le chiffrement symétrique du message et du code de hachage
Intégrité et **Authentification et non répudiation** : par signature numérique

---



Principe : on emploie une fonction de hachage mais aucun chiffrement pour l'authentification de message. La technique suppose que les deux parties communicantes partagent une valeur secrète commune S. A calcule la valeur de hachage à la suite de la concaténation de M et de S et ajoute la valeur de hachage résultante à M. Puisque B possède S, il peut recalculer la valeur de hachage à vérifier.
Intégrité : Puisque la valeur secrète elle-même n'est pas envoyé, un adversaire ne peut pas modifier un message arrêté et ne peut pas produire un message faux.
Authentification : par le secret s



Principe : Chiffrer le message entier et le code de hachage de M et de S.
Intégrité : comme le précédant
Authentification : par le secret s
Confidentialité par le chiffrement symétrique du message et du code de hachage