Authentification avec MAC et hachage

Saiida LAZAAR

Département Mathématiques Informatique
Université AbdelMalek Essaadi – ENSA de Tanger

Février 2019

Sommaire

Introduction

Ce cours présente un receuil de connaissances sur les fonctions de hachage qui garantissent l'intégrité des données échangées entre différentes entités sur les réseaux.

Le principal rôle étant de se protéger contre des attaques actives visant *à* falsifier les données interceptées, les détruire ou les crypter pour produire un ransomware.

Il aborde aussi l'authentification des messages et des correspondants par des procédés cryptographiques.

Introduction

L'authentification du message repose sur trois principes :

– La validation de l'identité du créateur du message
- La protection de l'intégrité d'un message
- La non-répudiation de l'origine (résolution de conflit)

Trois méthodes sont possibles :

– chiffrer le message
– utiliser une fonction de hachage
– utiliser un code d'authentification de message (MAC - Message authentication code)

Authentification

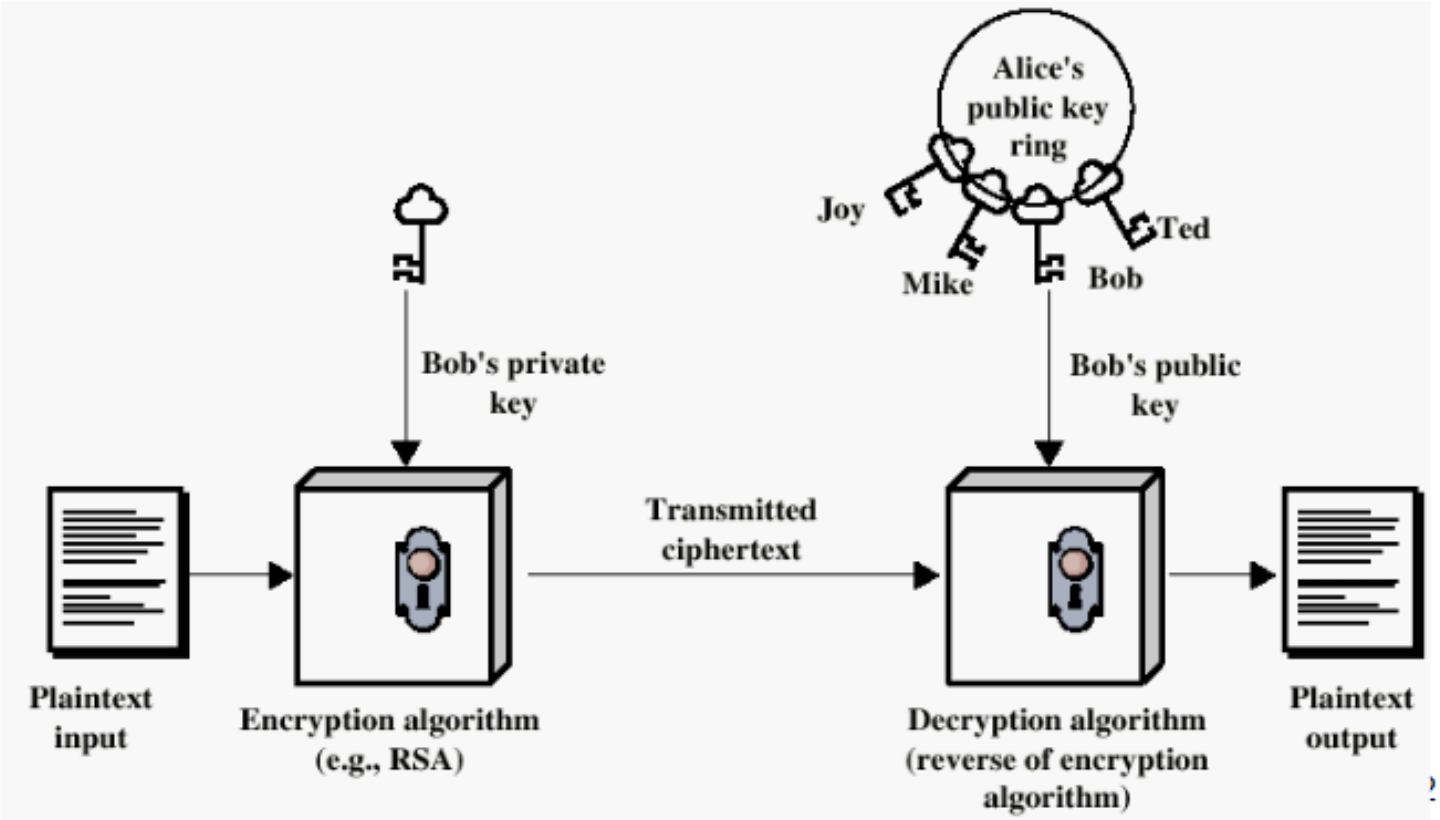
- Le chiffrement protège contre l'attaque passive (écoute)

- L'authentification du message protège contre l'attaque active.

- L'authentification permet de vérifier que les messages reçus sont authentiques et que la source est authentiques.

- Authentification avec chiffrement conventionnel *à* secrète + code de détection d'erreurs.

Authentification par RSA



Code d'authentification du message : Message Authentication Code

- Si Alice veut envoyer un message m, elle calcule $F(K, m) = MAC$ *où* K est une clé commune.
- Elle transmet le message et le MAC.
- Bob calcule son MAC et le compare avec le MAC reçu.

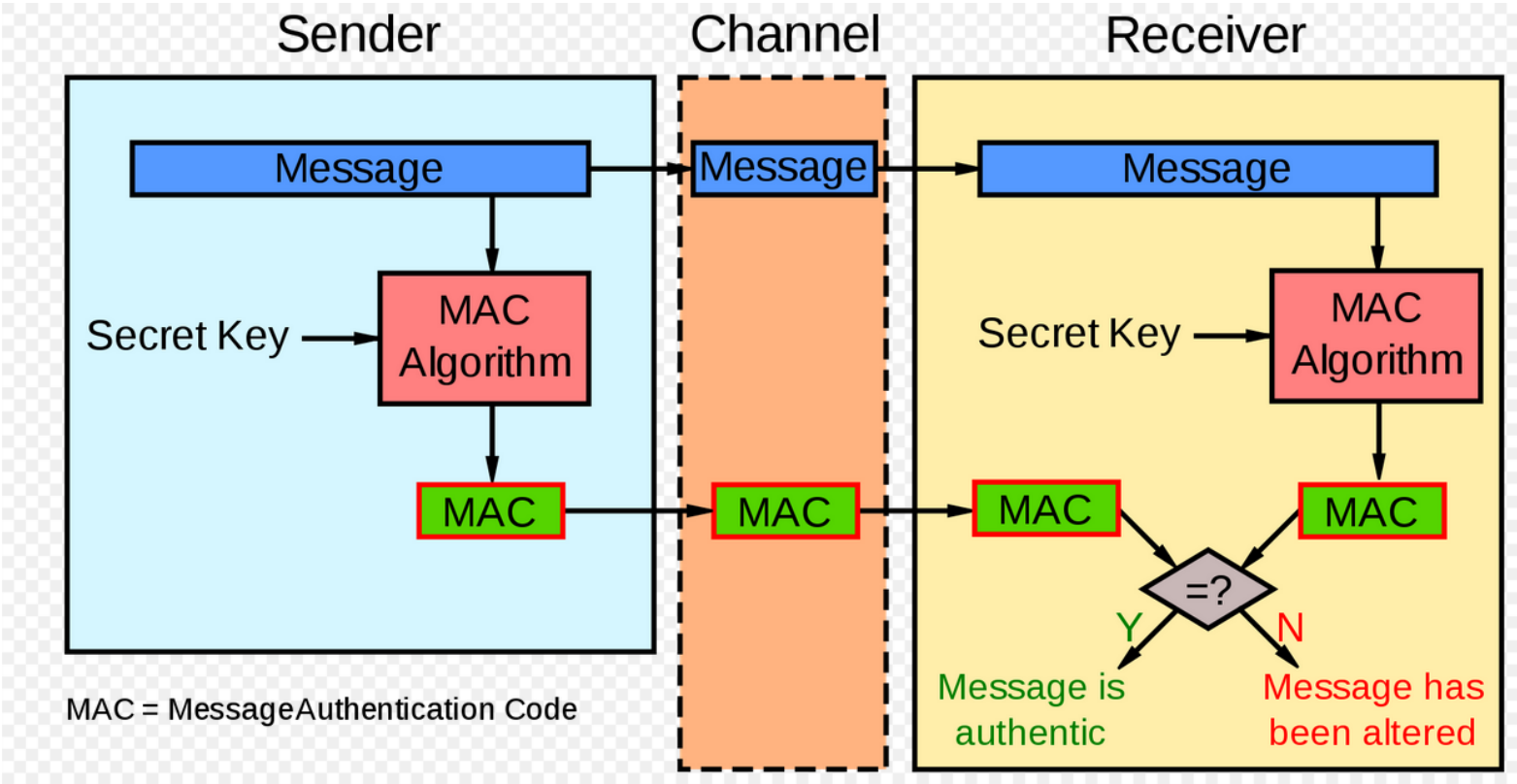


FIGURE – source wikipédia

Fonctionnement du MAC

- On utilise un algorithme de chiffrement par blocs, en mode CBC (chiffrement par chainage de blocs)
- On choisit un algorithme A_K dépendant de la clé K et chiffrant des blocs de n bits. Le message M est partagé en blocs de k bits : $m_1 \dots m_r$.
- On se donne un vecteur d'initialisation $v_0 = c_0$.
- On calcule successivement, et par récurrence, les chiffrés $c_i = A_K(c_{i-1} \oplus m_i)$.

Remarque : Tous les blocs chiffrés dépendent du précédent. Le dernier bloc chiffré dépend de tout le message (et pas uniquement du dernier bloc). **Ce bloc peut servir de MAC pour le message M.**

Intégrité : Fonctions de hachage à sens unique

Une fonction de hachage prend un message de taille variable et produit un résumé de taille fixe $H(m)$ sans utiliser une clé secrète.

Le résumé est envoyé avec le message, ce qui implique l'authentification du message.

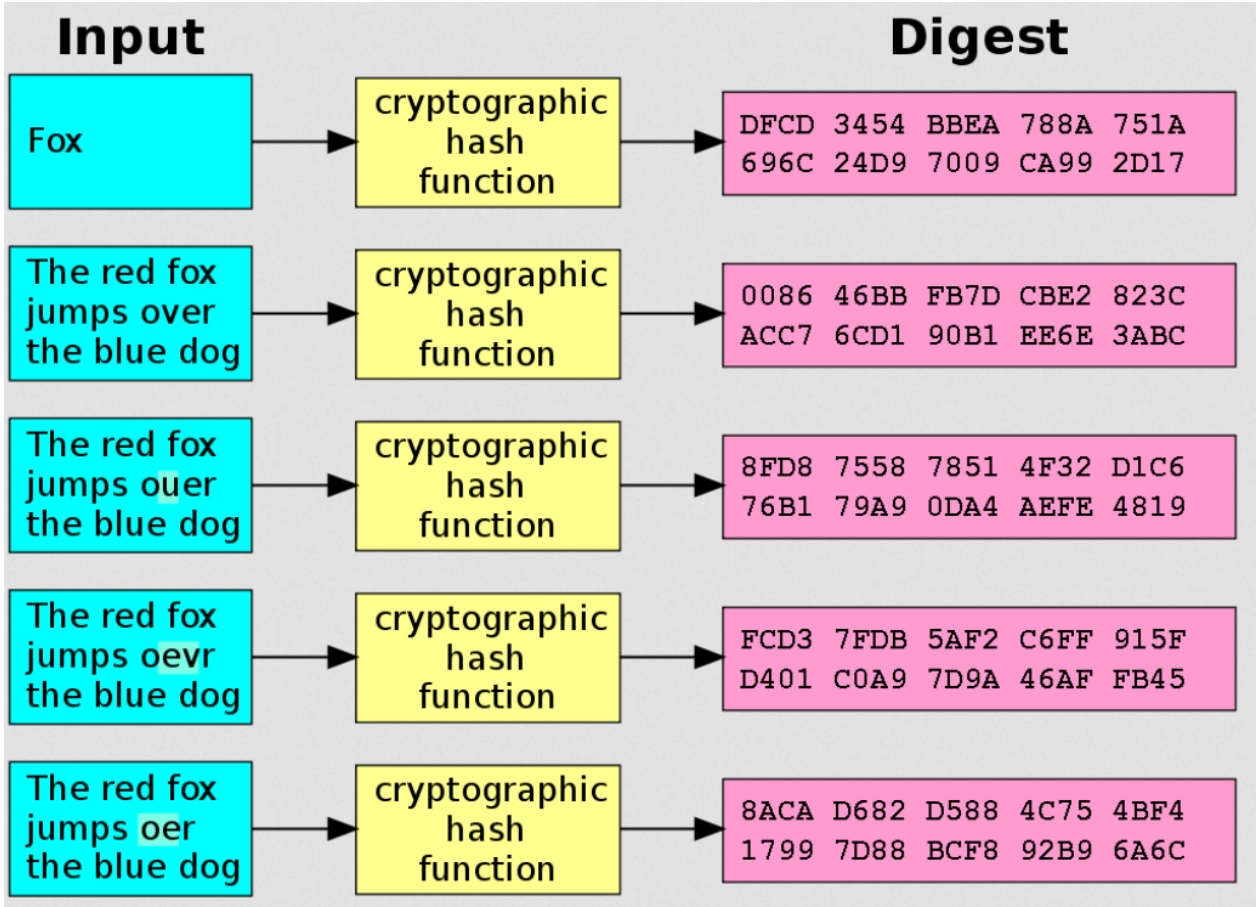
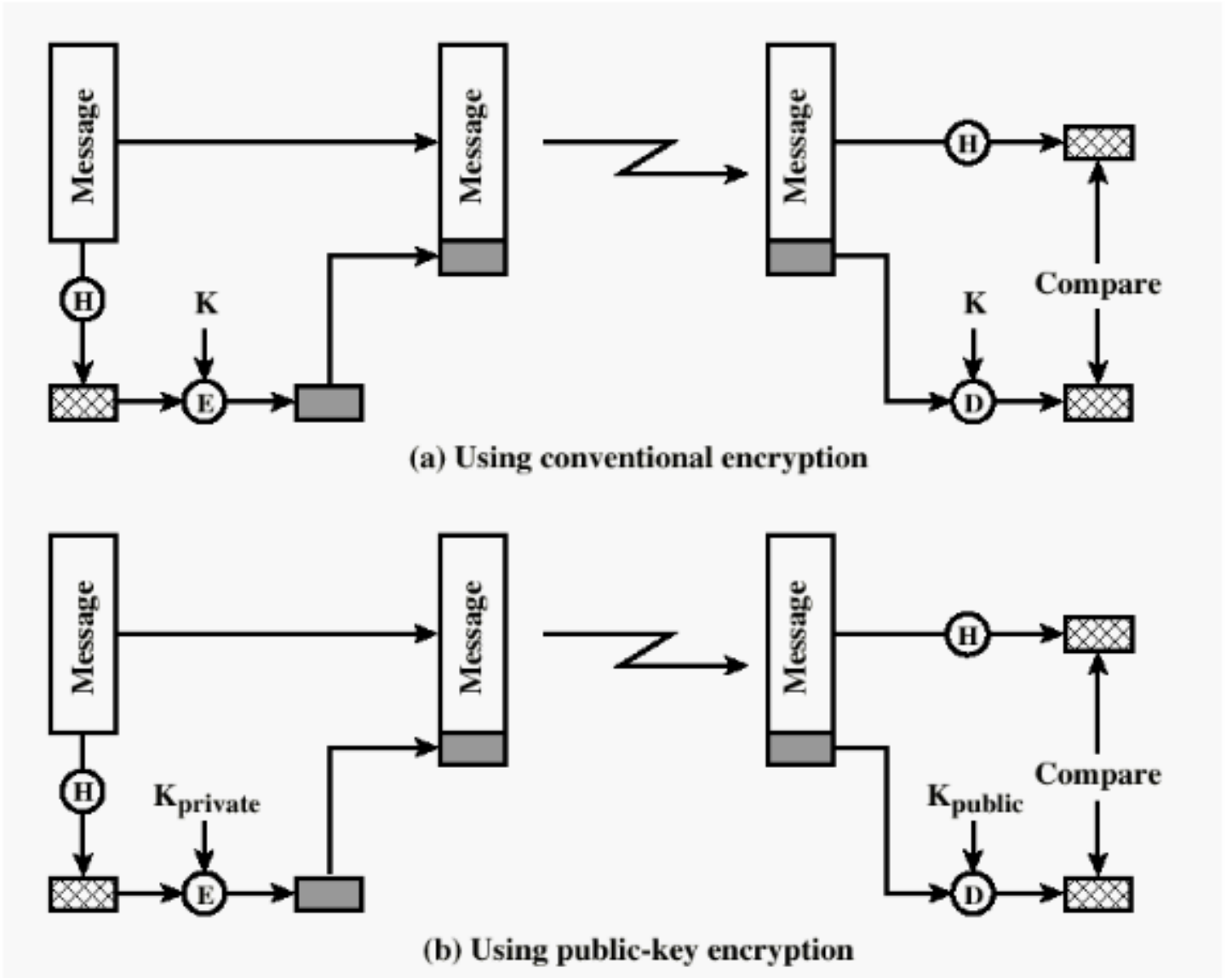


FIGURE – source wikipédia

Authentification avec Hachage et signature



Authentification X509

La recommandation X509 fait partie de la série X500 qui définit un service de répertoires (répertoire = Serveur + bdd avec nom, @, etc.)

Le répertoire contient le certificat à clé publique.

Le certificat contient la clé publique de l'utilisateur et il est signé par la clé privée d'une autorité de certification de confiance (voir cours SSL)

X509 est basé sur la cryptographie asymétrique et la signature digitale qui exige l'utilisation des fonctions de hachage.

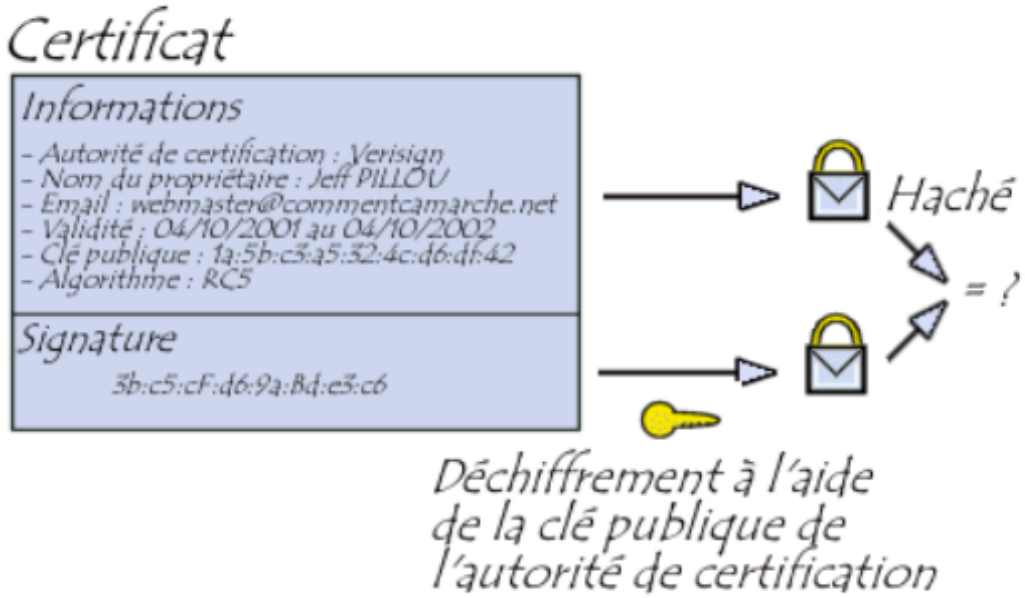


FIGURE – https ://www.commentcamarche.net

Exemples de fonctions de hachage

FIGURE – ....