Chiffrement asymétrique

1 - Pourquoi ne pas se limiter au cas symétrique

La méthode symétrique en équation :

mc = chiffrer(m, cle) où mc est le message chiffré et m le message.

m = dechiffrer(mc, cle) où mc est le message chiffré et md le déchiffré.

m = dechiffrer(chiffrer(m, cle), cle)

2 - Principe du chiffrement asymétrique

2.1 Principe des clés complémentaires : A et B

mca = chiffrer(m, cleA)

m = dechiffrer(mca, cleB)

m = dechiffrer(chiffrer(m, cleA), cleB)

m ≠ dechiffrer(chiffrer(m, cleA), cleA)

mcb = chiffrer(m, cleB)

m = dechiffrer(mcb, cleA)

m = dechiffrer(chiffrer(m, cleB), cleA)

m ≠ dechiffrer(chiffrer(m, cleB), cleB)

2.2 Principe des clés complémentaires : publiques et privées

mc_pub = chiffrer(m, pub)

m = dechiffrer(mc_pub, pri)

m = dechiffrer(chiffrer(m, pub), pri)

m ≠ dechiffrer(chiffrer(m, pub), pri)

2.3 Utilisation sur Internet ?

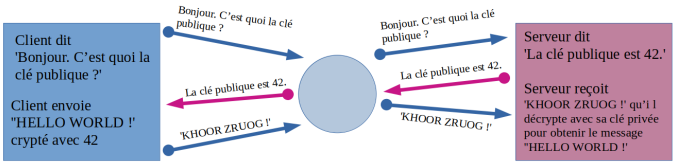

Figure 15.1 – Sur Internet ?

2.4 L'homme du milieu, une technique qui met à mal les solutions 1 et 2

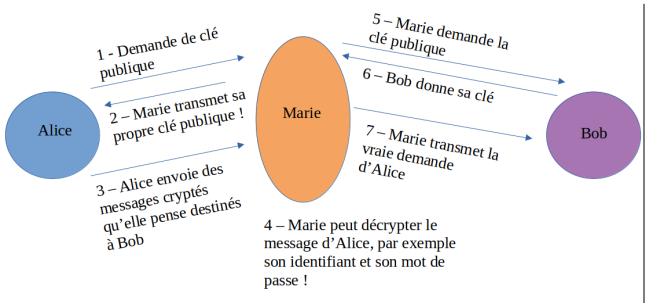

Figure 15.2 – Man In The Middle 1

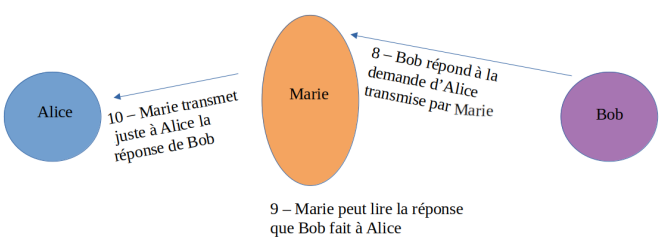

Figure 15.3 – Man In The Middle 2

3 - Le tiers de confiance et les certificats d'authentification

3.1 Principe du certificat

certificat = chiffrer("pubB et nom de domaine de B", priC)

dechiffrer(certificat, pubC) donne "pubB et nom de B"

3.2 Utilisation du certificat

Alice va donc calculer ceci :

dechiffrer(certificat, pubC)

= dechiffrer(chiffrer("pubB et nom de B", priC), pubC)

3.3 Les étapes

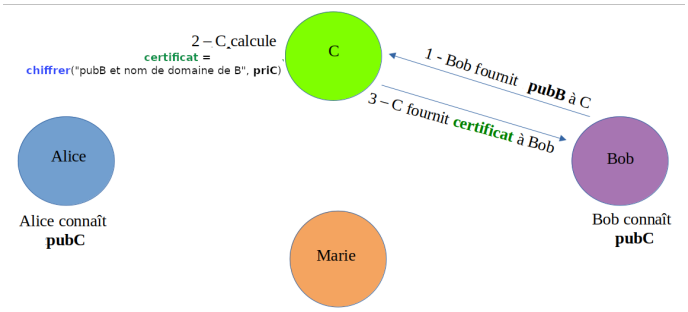

FIGURE 15.4 – Création du certificat

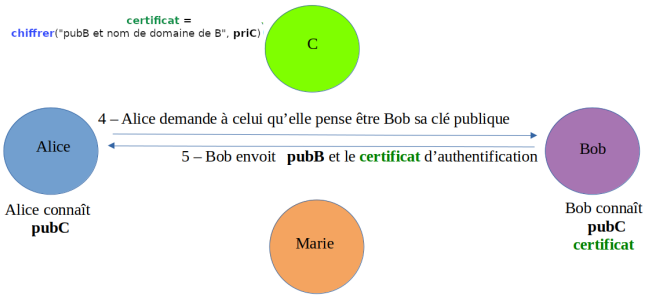

FIGURE 15.5 – Transmission du certificat

4 - HTTPS

- Un client dispose d'un navigateur Web disposant d'un ensemble de clés publiques correspondant aux organismes de certification auxquels les concepteurs du navigateur font confiance.
- Un serveur se déclare auprès de l'un des organismes de certification et lui demande de lui fournir un certificat d'authentification.
- Le client contacte le serveur en clair
- Le serveur lui transmet en clair sa clé publique et son certificat
- Le client vérifie la validité du certificat et de la clé publique
- Le client utilise alors la clé publique du serveur authentifié pour discuter avec le serveur de la méthode de chiffrement symétrique qu'ils vont utiliser lors de cette session de communication : quel algorithme et quelle clé de chiffrement symétrique.
- A partir de là, client et serveur peuvent communiquer de façon sécurisée en utilisant une méthode de chiffrement symétrique, moins gourmande en temps de calcul.