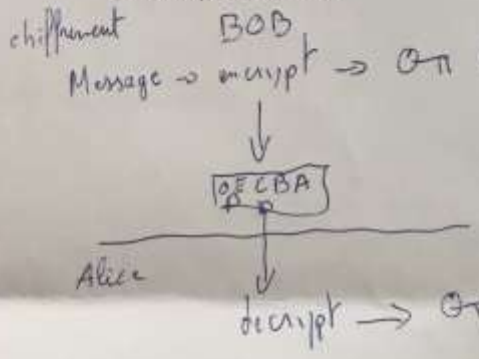
Nom : JUSSAN
Prénom : Charles

EPSI l'École d'ingénierie informatique

SÉCURITÉ DE L'INFORMATION ET DES ÉCHANGES
(I5)
interrogation n°1 – 20min

4. Les 2 applications principales de la cryptographie à clefs publique sont le chiffrement et la signature numérique. Expliquez comment fonctionnent ces deux applications dans le cas où Alice et Bob communiquent par e-mail.

chiffrement



Bob crypte le message avec sa clé publique et Alice ~~le~~ le message décrypte avec sa clé privée

Non

1,5

Signature électronique

Pour signer le message, pour indiquer que c'est bien bob qui a écrit ce message, bob utilise sa clé privée.

5,5

Nom : JUSSAN
Prénom : Charles

EPSI l'École d'ingénierie informatique

SÉCURITÉ DE L'INFORMATION ET DES ÉCHANGES

(I5)

interrogation n°1 – 20min

1. Rappelez et expliquez les 4 services de sécurité fournis par la cryptographie :

2

Authentification : Garantir au destinataire du message l'identité de l'expéditeur
Confidentialité : Garantir à l'expéditeur que seul le destinataire peut lire le message
Intégrité : Garantir l'exactitude et l'exhaustivité du message
Non répudiation : Garantir au destinataire que l'expéditeur ne pourra nier avoir envoyé le message

2. Expliquez les différences entre la cryptographie symétrique et à clef publique :

pas mal pas mal

Il existe la cryptographie symétrique par flux ou par bloc.
Flux : le message est chiffré bit à bit (octet par octet) à l'aide de la clé de chiffrement, le message est xoré
bloc : On découpe le message en bloc de taille identique
On chiffre chaque bloc et on utilise un mode d'opération
- ECB (Electronic Code Book)
- CBC (Cipher Bloc Chaining)

3. Donnez moi le nom de deux algorithmes de chiffrement symétrique :

2

Il existe l'algorithme RC4 pour le chiffrement par flux et l'algorithme DES en 64bits et AES en 128 bits