Exercice

Cet exercice porte sur l'utilisation des chiffrements symétrique et asymétrique.

Bob souhaite envoyer un message confidentiel à Alice sans qu'un espion, Marley, ne puisse le lire ou le modifier. Pour cela, il envisage plusieurs méthodes de chiffrement et de signature numérique.

Questions

1. Bob envisage d'utiliser un chiffrement symétrique pour sécuriser son message.

a. Bob rédige le `message.txt` et le chiffre pour obtenir `message.enc` puis il envoi le fichier ce dernier fichier à Alice. Expliquer pourquoi Alice ne pourra pas déchiffrer le fichier `message.enc`.

b. Citer deux avantages du chiffrement symétrique.

c. Quel est le plus grand inconvénient du chiffrement symétrique ?

2. Afin d'améliorer la sécurité de la communication avec Alice, Bob découvre le chiffrement asymétrique. Bob et Alice ont tous les deux généré une clé publique (`KeyPubAlice.pem` et `KeyPubBob.pem`) et une clé privée (`KeyPrivAlice.pem` et `KeyPrivBob.pem`)

a. Quelle est la différence entre clé privée et clé publique ?

b. Citer un avantage du chiffrement asymétrique.

c. Bob chiffre le fichier `message.txt` avec sa clé puplique. Il obtient le fichier `message.enc` qu'il envoie à Alice. Expliquer pourquoi Alice n'arrivera pas à déchiffrer le fichier `message.enc`

d. Bob a enfin réussi à chiffrer correctement : `message.txt` en `message.enc`. Expliquer comment Alice doit procéder pour déchiffrer le message.

e. Maintenant Bob souhaite transmettre un diaporama à Alice. Malheureusement, le chiffrement asymétrique ne fonctionne pas. Expliquer pourquoi.

f. Bob a compris son erreur et la démarche qu'il a entrepris pour pouvoir envoyer son diaporama de façon sécurisé :

Il met un mot de passe dans un fichier `password.txt`. Il chiffre ce fichier avec la clé publique d'Alice. Il obtient alors un fichier `password.enc`. Puis Bob rédige un fichier `diaporama.pdf` et le chiffre avec une chiffrement symétrique pour obtenir `diaporama.enc`

i. Quels sont les fichiers qu'il doit transmettre à Alice ?

ii. Comment Alice va t-elle faire pour déchiffrer le fichier `diaporama.enc` ?

g. Attaque 1 : Marley intercepte le fichier `password.enc`. Peut-il retrouver le mot de passe choisi par Bob ?

h. Attaque 2 : Marley a aussi intercepté le fichier `diaporama.enc`. Peut-il déchiffrer ce fichier ?

i. Attaque 3 : Marley a aussi intercepté la clé privée de Bob. Peut-il maintenant déchiffrer le fichier `diaporama.enc` ?

j. Attaque 4 : Quelle idée donner à Marley pour l'aider à déchiffrer les messages (qu'il aurait interceptés) échangés par Bob et Alice ?