1. (0.25pts) Générer une clé privée RSA pour Alice tout en la chiffrant avec triple DES (des3) en utilisant un mot de passe comme clé symétrique. La clé RSA générée devrait être mise dans le fichier alice-privatekey.pem.

Pass phrase = motdepasse

Text

Description automatically generated

Text

Description automatically generated

1. (0.25pts) Extraire la clé publique de Alice et la mettre dans le fichier alice-publickey.pem

Text

Description automatically generated

Text

Description automatically generated

1. Faire la même chose pour Bob pour lui générer une paire de clés et les mettre dans bob-privatekey.pem et bob-publickey.pem.

Pass phrase = passedemot

Text

Description automatically generated

Text

Description automatically generatedText

Description automatically generatedText

Description automatically generated

1. Créer un fichier message.txt dans lequel vous écrivez votre nom et votre prénom.

Graphical user interface, text, application

Description automatically generated

1. (0.5pts) Montrer, via une capture d’écran, les opérations openssl qu’Alice fait pour envoyer message.txt haché avec SHA1 et signé avec sa clé privée.

Text

Description automatically generated

Text

Description automatically generated

1. (0.5pts) Montrer, via une capture d’écran, les opérations openssl que Bob fait pour vérifier la signature.



1. Pour qu’Alice envoie message.txt d’une manière confidentielle à Bob, il exécute les étapes suivantes :
   1. (0.25pts) Alice génère une clé aléatoire et mets le résultat binaire dans le fichier key.bin.



* 1. (0.25pts) Alice chiffre message.txt avec key.bin en utilisant AES-128-CBC et met le résultat dans protected-message.txt codé en base64.

Text

Description automatically generated

* 1. (0.5pts) Alice chiffre, en utilisant rsautl, la clé key.bin avec la clé publique de bob et met le résultat dans protected-key.bin

1. (0.5pts) Aider Bob à retrouver le contenu de message.txt à partir de protected-key.bin et protected-message.txt. Montrer les étapes de calculs, via des captures d’écran openssl, ainsi que le message.txt obtenu une fois le calcul terminé.