Problem Set 2: Cryptography

Each student should submit his own report: NO TEAM work.

Due date: 11:59PM Eastern, February 10th, 2013.

Late submissions will result in a 10% penalty per day (e.g., 2.5 days late result in 25% penalty)

1. Application of Cryptography

Write a Java application that can be used to encrypt and sign a file to be sent by email. The sender knows the public key of the destination, and has a private key to sign the file. The application can also be used by the receiver to decrypt the file using his private key and to verify the signature using the public key of the sender. Design the application to be efficient (i.e., use a combination of public key crypto and symmteric key crypto). Design and implement your own application. Justify the use of key sizes, algorithms and modes.

For the implementation part, you can use the Sun JCE crypto-library (http://java.sun.com/products/jce/) or Bouncy Castle (http://www.bouncycastle.org/index.html). Please refer to the sample java code for a starting point about JCE (remember that DES is considered insecure today).

The application should operate as follows. For encryption and signatures:

- java fcrypt -e destination_public_key_filename sender_private_key_filename input_plaintext_file output_ciphertext_file

and for decryption and signature verification:

- java fcrypt -d destination_private_key_filename sender_public_key_filename input_ciphertext_file output_plaintext_file