CS6740 NETWORK SECURITY

PS-2

INSTALLATION/USAGE INSTRUCTIONS

Arpit Mehta

Overview:

This is an application to encrypt and sign the contents of a plaintext file to be sent by email. The sender knows the public key of destination, and has his/her private key to sign the file. Thi application can also be used by a receiver to decrypt the contents of a ciphertext file using his/her private key and verify the signature using the public key of the sender.

Encryption Process:

Sender encrypts a message using Advanced Encryption Standard (AES). The sender uses a destination public RSA key to encrypt an AES key. Finally, the AES key is shared with the destination using the concepts of asymmetric key cryptography. The AES key is wrapped with the destination public key and (Encrypted AES key, ciphertext) bytes are hashed and signed with the sender's RSA private key.The RSA key pairs are generated using the RSAKeyGen application. Standard 1024 bit RSA keys are used for RSA.

Decryption Process:

Destination user, who reads the contents of the ciphertext file, first verifies the signature of the sender. Once the signature is verified, it proceeds to Unwrap the AES key by using its private key. Then it proceeds to decrypt the ciphertext using the AES key.

Parameters:

RSA uses the standard 1024 key length, and is generated by the RSAKeyGen.java.

AES uses the default key size (256 bits) with CBC mode of encryption. This is because CBC mode is more secure than ECB.

Signature verification is done with SHA1WithRSA. SHA1(AESKey + ciphertext) is used as the signature.

To execute the program use the following commands:

Encryption:

```
-e publicKey.key privateKey.key plaintext.txt ciphertext.txt
```

Decryption:

```
-d privateKey.key publicKey.key ciphertext.txt plaintext.txt
```