PS2 Application of Cryptography

```
java fcrypt -e destination_public_key_filename sender_private_key_filename input_plaintext_file output_ciphertext_file
```

- For the above input, program creates a pair of keys using RSA for a sender and a receiver. And also stores them in a file.
- It renames the corresponding file according to the given file names.
- It creates plain text file with the same name as that of a given input and writes plaintext.
- Program then follows following encryption algorithm.

Encryption Algorithm :

1. Read the plain text.

2. sign the plain text using private key of the sender that gives signature.

3.Generate symmetric key using AES.

4.Encrypt the plain text using symmetric key that produces cipher text.

5.Encrypt the symmetric key using public key of the destination that gives encrypted key.

6.Write cipher, signature, encrypted key into the cipher file.

```
java fcrypt -d destination_private_key_filename sender_public_key_filename input_ciphertext_file output_plaintext_file
```

- For the above input, program renames the already created files according the given file names.
- Program then follows following decryption algorithms

Decryption Algorithm :

1.Read the encrypted key.

2.Decrypt this key using sender's public key and get the symmetric key.

3.Read the cipher text.

4.Using symmetric key decrypt cipher text and get the plain text.

5.Read the signature.

6. Verify signature using plain text and public key of the sender.

7. Creates plain text file and writes the plain text in the output file.

Algorithms used

- Asymmetric key algorithm i.e RSA is implemented to encrypt/decrypt symmetric key. RSA algorithm produces public and private keys. Destination's public key is used to encrypt symmetric key and private key is used to decrypt it. RSA is mainly used for encryption and decryption of keys, since it solves the problem of key distribution.
- Symmetric key algorithm i.e AES 128 bit is implemented to encrypt /decrypt message between sender and receiver where sender and receiver uses shared/secret key for encryption and decryption. Symmetric key algorithm are faster compare to asymmetric key algorithm. Thus for encryption and decryption of data AES is used.
- Digital signature Algorithm i.e MD5withRSA is implemented to sign/verify the message. Keys produced during RSA implementation are used for digital signature. In this algorithm, hash of the message is signed with sender's private key. And message is verified at destination using signature, original message and the public key of the sender. Digital signature specifies the authenticity of message. By verifying digital signature receiver can ensure that message was created by known sender.

Key sizes

- Key size is directly proportional to security. In cryptosystems, key length is measured in bits and each bit of a key increases the difficulty of a brute-force attack exponentially. A key should therefore be large enough that a brute force attack is infeasible – i.e., would take too long to execute. However each bit slows down the cryptosystem.
- As each cryptographic system have different cryptographic complexity, it is usual to have different key sizes for the same level of security, depending upon the algorithm used. For example, the security available with a 1024-bit key using asymmetric RSA is considered approximately equal in security to an 80-bit key in a symmetric algorithm.
- In PS2 RSA is implemented for both sender and receiver having key size is 1024 bits,2048 bits respectively.
- For asymmetric cryptography such as RSA, some piece of information is disclosed (the public key) that is related to the decryption key(the private key). Because of this, the larger key sizes are necessary so that it is not easy to get private key from public key.

- In PS2 AES is implemented to transfer actual message between sender and receiver. The key size for the same is 128 bits which is considered very strong. This is a shared/secret key between the sender and the receiver.

Mode of operations

- There are two major types of ciphers: *block* and *stream*. Block ciphers process entire blocks at a time, usually many bytes in length. In contrast, stream ciphers process incoming data one small unit at a time.
- When encrypting using a simple block cipher, two identical blocks of plaintext will always produce an identical block of cipher text. Thus it is easy to break the cipher text if someone note the blocks of repeating text.
- In order to add more complexity to the text, feedback modes use the previous block of output to alter the input blocks before applying the encryption algorithm.
- In PS2 RSA does not use mode of operation typically because, RSA is used to encrypt an AES key. But AES uses CBC (cipher block chaining) mode where each block of plaintext is XORed with the previous cipher text block before being encrypted. The first block needs an initial value, and this value is called the initialization vector (IV). That Iv is also sent to the receiver as receiver needs it while decrypting the cipher text.