Data Security Project

Message Exchange - Hybrid Cryptographic Scheme

The project utilizes 2 Java programs, one acting as server (or receiver), and the other acting as client (or sender).

Server (or receiver) design

The server has following features:

1. Generate public and private keys using El Gamal algorithm
2. Export public key for use by client
3. Receive both AES key and cipher message from client (exchanged using files)
4. Recover AES by decrypting using private key
5. Recover message by decrypting using AES key.

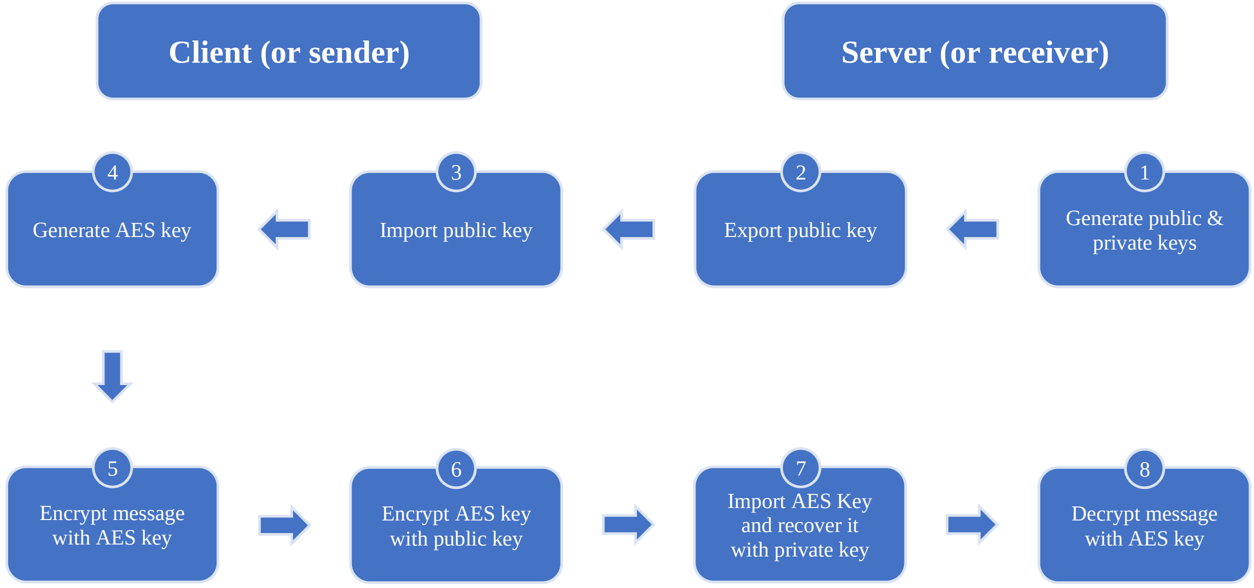
The server allows customization of El Gamal public / private with a choice of key size - 128, 256, 512, 1024, 2048 (bits).

Client (or sender) design

The client has following features:

1. Generate AES key
2. Import public key
3. Encrypt AES key with public key
4. Encrypt message with AES key for transmission to the server (exchanged using files)
5. Export AES key for transmission to the server (exchanged using files) along with AES algorithm and mode, and initialization vector (IV) for each mode

The client allows customization of AES key with a choice of key size - 128, 192, 256, mode of operation (block type), and password for AES key.


Client (or sender)
Server (or receiver)
1
Generate public & private keys
2
Export public key
3
Import public key
4
Generate AES key
5
Encrypt message with AES key
6
Encrypt AES key with public key
7
Import AES Key and recover it with private key
8
Decrypt message with AES key