**Explaining the Source code structure**

All the source files are contained in the folder Hybrid Cryptosystem.

Inside the folder, we have two sections namely cryptosystem and cryptoattack.

**Crypto System:**

Crypto system contains the java files implementing the Hybrid Cryptosystem. RSA encryption and decryption, AES encryption and decryption is implemented in our case.

The main execution for the crypto system is at “MainSystem.java”. So, this file is where we have to get in, to start the execution for cryptosystem.

Individual files “AESEncryption.java” and “RSAEncryption.java” contain the source code for encryption and the decryption for their respective schemes. But when the execution is started at “MainSystem.java”, the java files are called according to the flow.

**Crypto Attack:**

Crypto attack contains the java files to successfully perform an attack on the hybrid system. The basic assumption is that the attacker knows the values of N, e as they are public and are available to everyone. Additionally, we assume that the attacker has eavesdropped through the communication channel and has managed to get the values of “Encrypted Key” and the “Cipher Text”. So, with these information, the attacker will be able to decrypt the key and also decrypt the plain text. We have included the cube root attack as well as square root attack as a part of the crypto attack module.

The execution point for the Crypto attack module starts at “AttackSystem.java”. The “PrimeFactorization.java” contains the logic for finding out the values of p and q when N is available. When the attacker enters all the necessary data, the system successfully decrypts the message.