**Crypto Chat Server & Client**(Jonas Höing, Philipp Klaas)

Funktionalitäten Server:

* Server lauscht auf definiertem Port auf eingehende Verbindungen
* Nach Aufbau einer eingehenden Verbindung wartet der Server auf eine „Key Exchange Request“-Anfrage vom Client.
* Server generiert bei Key Exchange Request ein asymmetrisches RSA Key Pair (1024 bit) und übermittelt PublicKey an Client.
* Server wartet auf Übermittlung eines mit dem PublicKey verschlüsselten SecretKey, welcher dann (nach Entschlüsselung mit PrivateKey) als SecretKey für die Verschlüsselung der Nachrichten verwendet wird.
* Nach dem KeyExchange können mit dem Server Nachrichten verschlüsselt empfangen und gesendet werden.

Funktionalitäten Client:

* Client kann nach Eingabe des Hostnames + Port des ChatServers eine Verbindung zum Server aufbauen und initiiert einen Key Exchange.
* Client wartet auf und empfängt PublicKey vom Server.
* Client erzeugt symmetrischen Secret Key mittels AES (128 bit) und verschlüsselt diesen mittels PublicKey des Servers.
* Client sendet verschlüsselten Secret Key an Server und schließt damit den Key Exchange ab.
* Nach dem Key Exchange können mit dem Client Nachrichten verschlüsselt empfangen und gesendet werden.

**Beispielnutzung:**

1. Start des Servers

java -jar CryptoChatServer.jar

1. Start des Clients

java -jar CryptoChatClient.jar

Zusätzlich haben wir auch noch in der LokalCryptoViaFile.jar den Schlüsselaustausch mittels File und Austausch des verschlüsselten Strings mittels File implementiert.