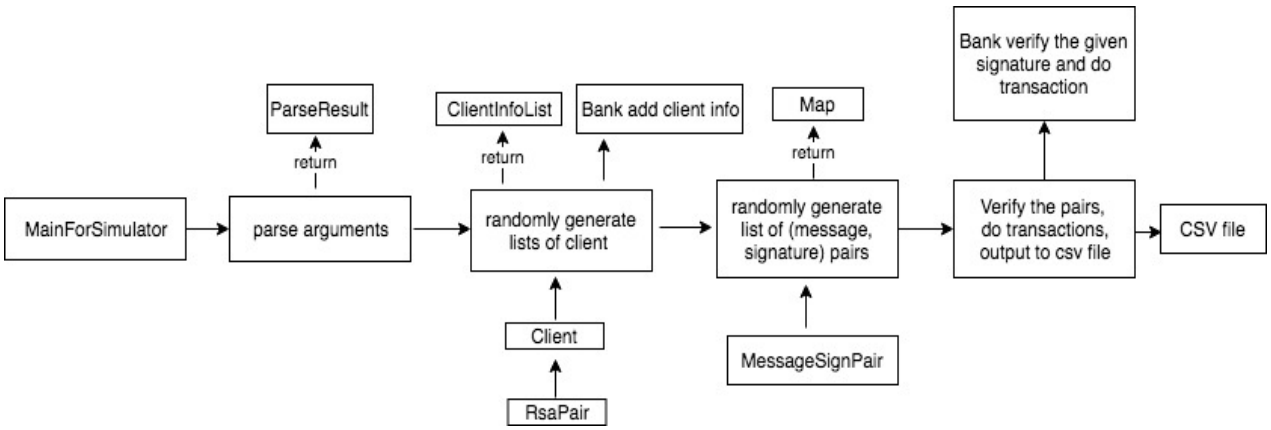
# Assignment10 Design Report

1. General Introduction:
The design mainly includes the following functional classes:

| class | Desciption |
|---|---|
| SecureBankVerificationSimulator | parse the command line arguments the user inputs; generate list of clients; generate list of (message, digital) signature pairs; write to output csv |
| RsaPair | generate and store the RSA pair |
| MessageSignPair | generate and store a (message, digital) signature pair |
| Bank | store the client information (ID, client public keys, withdrawal/deposit limit); verify client signature; do transaction |
| MainForSimulator | this is the entry point of the java program and enables users to type in command line arguments |

In addition, I have several classes designed for storing the intermediate information produced by some classes, including Client, ClientInfoList, Key and ParseResult.

2.Work Flow:




3.Handling special requirements:

- The SecureBankVerificationSimulator will parse the arguments, randomly create the requested number of clients and unique (message, signature) pairs. To deal with the cases if the same client has multiple (message, signature) pairs, I store the information in a map with client ID as a key, and list of pairs as the value.
- To generate the requested number of unique pairs, the percentage of incorrect message parameter has been taken into consideration.
- Bank has no access to client's private keys. The information about client's deposit limit and withdrawal limit are only known to the bank.
- BigInteger and SecureRandom have been used in the process of RSA key generation, digital signature generation and signature verification.