**Documentation**

**Encryption**

Inputs

The program takes two inputs: A configuration file and a data file.

The configuration consists of all encryption parameters-

String password;  
String alias;  
String keyStorePath;  
String signature;  
String signAlgorithm;  
int keyLength;  
String cipherProvider;  
String signatureProvider;  
String encryptedSymmetricKeyString;  
String IVString;  
String cipherToEncryptSymmetricKey;  
String cipherTpEncryptData;

For example a path and password to a keystore, desired ciphers and providers, a place holder for the symmetric key the encryption will generate (and encrypt), etc.

The data file is the .txt file that we would like to encrypt.

Algorithms Used

Generating SecureRandom- SHA1PRNG

Generating symmetric key - AES

**Decryption**

Uses the algorithm used in the encryption as inputs.

APIs

X509Certificate .getKey

KeyStore.getInstance

KeyStore.load

KeyStore.getKey

KeyGenerator. .generateKey

Cipher.getInstance

Cipher .init

Cipher.doFinal  
SecureRandom.getInstance

Signature.getInstance

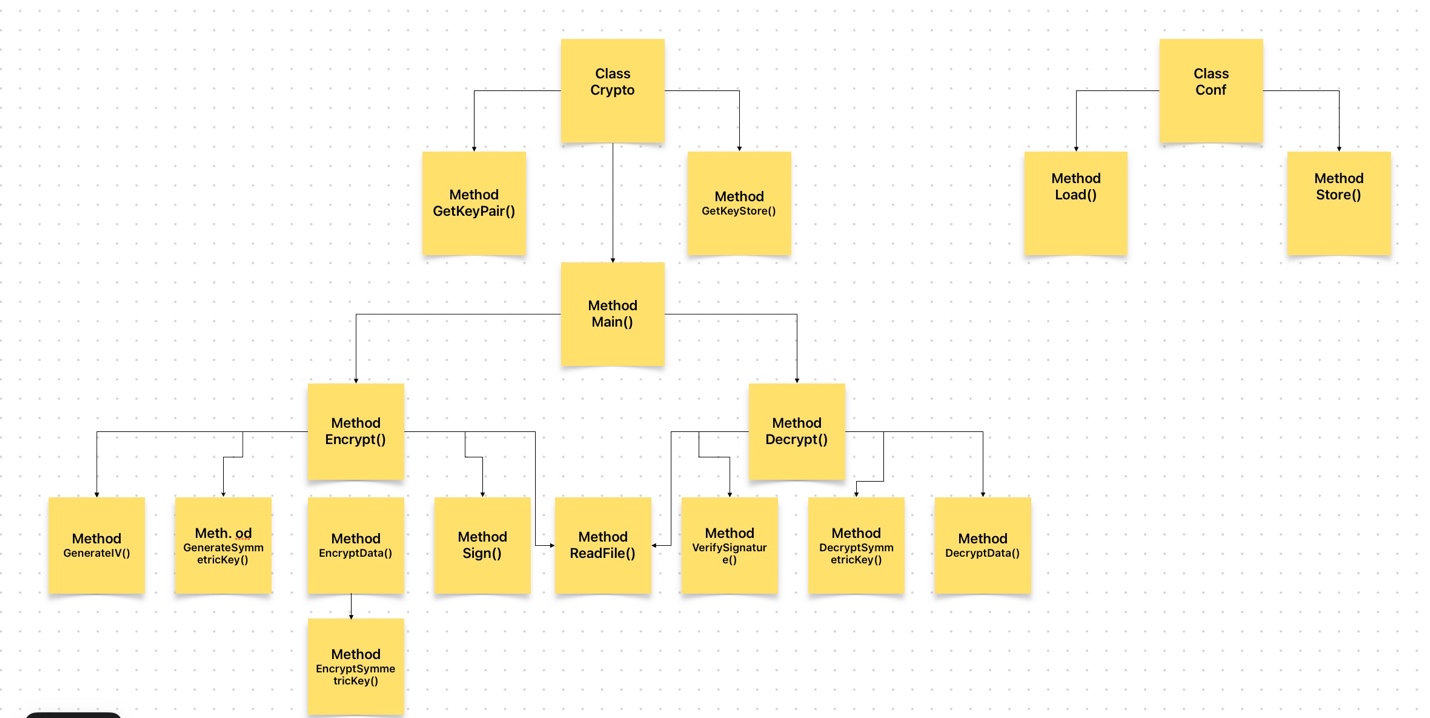
Signature. initSign

Signature.update

Signature.sign

Signature .initVerify

Class diagram



How to run:

javac Conf.java

javac Crypto.java

java Crypto.java conf.txt plaintext.txt <Keystore password>