Cryptography Homework #1 Report

I tested all the algorithm in main class. I'll share all the test values next part as screenshots.

- Used IntelliJ IDEA as an IDE.

- Used JAVA language for the implementation.

- Used BigInteger class in the implementation. This class in Java used for mathematical operation which involves ver big integer calculations that are outside the limit of all available primitive data types.

- ExtendedEuclideanAlgorithm class has 4 methods. findGcdXAndY method gives us gcd, x and y using values a and b according to ax + by = gcd(a,b) findGcdOfTwoNumber method gives us only gcd. We can check two numbers are prime using areRelativelyPrime method. We can find Multiplicative inverse of a number in modular arithmetic using findMultiplicativeInverse method.

- FermatLittleTheoremClass has two methods. These methods are generateRandomCoPrimeNumber and fermatMethod. The one of the important thing in here is iteration number. If iteration number is increased, we'll get more certain result. However, execution time can be increased.

- FastModularExponentiation class contains 4 methods. Thanks to this algorithm, we can compute a^b % p.

- AES class implements AES algorithm for encryption and decryption operations. This class contains 3 important methods. RandomKeyGenerator generates random 256-bit key for every encryption&&decryption pair. Encrypt method uses initial vector because of cipher block chaining. From the initial vector, we created IvParameterSpec which is required when creating the cipher.

- In main class, I created objects in order to test algorithms calling the methods. I'll share my screenshots. In addition, I wrote comments in every classes so that can be understand easily.

SCREENSHOTS