

C/C++ code for Encryptosystem

1. GCD (a,b)

User input two numbers a & b and the system returns there Greatest Common Divisor otherwise mentions if they are co prime.

2. Inverse (n,m) / Extended Euclidean Algorithm

User input two numbers n & m, where n is the number whose inverse is to be calculated and m is the modulus. System should return calculated inverse or update user if no inverse exists.

3. Miller Rabin Test (p)

User should enter p as input to see whether p is a prime number or a composite number? System should test p for at least 10 different a's and then return "Number is Prime" or "Number is not prime" for the given input.

4. Advanced Encryption Standard (AES).

5. Ron Rivest, Adi Shamir (RSA) cryptosystem

(via Miller-Rabin- Test + EEU). pseude-code from Wikipedia with same Variable Name

6. Mathematical operation on infinitely Extra Large Number