Review for Test 3

Know the following definitions:

primitive roots

Carmicheal number

order of an element in a group

Eulers phi function

Know:

How to encrypt or decrypt with Vigenere cipher

How to do the extended Euclidean algorithm

How to exchange a key (Diffie Hellman) elliptic or regular

Know how to make the lists in Giant Step Baby Step

Prime number theorem and how to use it

Legendre/Jacobi symbol calculations - quadratic reciprocity

elliptic curve discrete log problem

RSA digital signature

Main Algorithms to Know

Elliptic Curve Addition P+Q or P+P

Polig Hellman (and Chinese Remainder)

Difference of Squares

Index Calculus

Miller Rabin

Not on Test

Pollard's algorithm

Micali Goldwasswer

DSA