LABORATORY 1

INRODUCTION TO CRYPTOGRAPHY

SEMESTER 2, 2013/14

GROUP MEMBERS:

NAME	METRIC NO

SECTION:

DATE:

INSTRUCTOR SIGNATURE:

At the end of the laboratory work, student will be able:

i. To evaluate mathematical expression based on modulo arithmetic.
ii. To apply Euclid Algorithm in calculating the Greatest Common Divisor of two given numbers,
iii. To apply Extended Euclid Algorithm in calculating the multiplicative inverse of a given number.
iv. To evaluate the Euler Totient Function, $\phi(n)$.

A. Modulo Arithmetic

Change each of group member metric numbers to modulo 313.
Example: Metric Number = 098765 = 98765 mod 313

X = Metric Number 1 =

Y = Metric Number 2 =

Z = Metric Number 3 =

1. $X + Y$

2. $X - C$

3. $(X + Y) \times Z$

4. Find Y^{23}

B. Euclid's Algorithm

Change each of the group member metric numbers to two different numbers of *a* and *n*..
Example: Metric Number = 098765, therefore (*a*, *n*) = (987, 65)

X = Metric Number 1 =

Y = Metric Number 2 =

Z = Metric Number 3 =

i. Find gcd of *X*

q	***r*1**	***r*2**	***r***

Ii Find gcd of *Z*

q	***r*1**	***r*2**	***r***

C. Extended Euclid's (or Binary GCD) Algorithm

Use the same numbers in (B) for the following questions.

Identify the multiplicative inverse of *X, Y* and *Z.* Prove all the answers.

D. Fermat's Theorem and Euler's Generalization

Find the multiplicative inverse by applying Fermat's Theorem and/or Euler's Generalization.

1. $8^{-1} \bmod 77$

2. $7^{-1} \bmod 15$

3. $60^{-1} \bmod 187$

4. $71^{1} \bmod 100$