Roll No. | | | | | | | | |

Gautam Buddha University

Mid Semester Examinations

M.Sc. Applied Mathematics First Semester, (September, 2013)

Course Name: Foundation of Cryptography and Security — Maximum Marks: 50
Course Code: MA-008 — Time: 2:00 Hours

NOTE: Attempt **all** the questions. Be concise and adopt mathematical approach.

Q.**1.** Attempt ALL parts of the following: $(5 \times 2 = 10)$

(a) Find gcd(174, 204).

(b) Find all the integral solutions of $174x + 204y = 18$.

(c) If $d = gcd(a,b)$, then what is the gcd of a^n and b^n? What will be the gcd of a^m and b^n?

(d) Encrypt MID SEMESTER EXAMINATIONS by using Caeser Cipher system.

(e) Do the cryptanalysis of the message "ilza vm sbjr" (without quotes).

Q.**2.** Attempt ALL parts of the following: $(2 \times 5 = 10)$

(a) Describe Euclid's Algorithm. If $a = 66$ and $b = 26$ then find $gcd(a,b)$ and also express the $gcd(a,b) = ax + by$

(b) Show that there are infinitely many primes.

Q.**3.** Attempt ALL parts of the following: $(2 \times 5 = 10)$

(a) State the Chinese Remainder Theorem. Solve the following system of linear congruences $x \equiv 2 \mod 6$, $x \equiv 1 \mod 5$, $x \equiv 3 \mod 7$.

(b) Solve the system of linear congruences $5x \equiv 1 \mod 6$, $3x \equiv 2 \mod 5$, $4x \equiv 5 \mod 7$.

Q.**4.** Attempt ALL parts of the following: $(2 \times 5 = 10)$

(a) Define a cryptosystem. What are symmetric cryptosystems and asymmetric cryptosystems?

(b) What is the Key Management Problem? What are the known possible solutions?

Q.**5.** Attempt ALL parts of the following: $(2 \times 5 = 10)$

(a) What do you understand with attacks. Describe various attacks. (You may take help of diagrams if required.)

(b) Describe Diffie-Hellmen Key agreement protocol? Also show that this is insecure against Man-in-Middle Attack?