MERU UNIVERSITY OF SCIENCE AND TECHNOLOGY

P.O. Box 972-60200 – Meru-Kenya
Tel: +254(0) 799 529 958, +254(0) 799 529 959, + 254 (0) 712 524 293,
Website: info@must.ac.ke Email: info@must.ac.ke

University Examinations 2022/2023

FIRST YEAR SECOND SEMESTER EXAMINATION FOR THE DEGREE OF MASTER OF SCIENCE IN PURE MATHEMATICS

SMA 6010: INTRODUCTION TO MATHEMATICAL CRYPTOGRAPHY

DATE: AUGUST 2023 **TIME: 3 HOURS**

INSTRUCTIONS: *Answer any **three** questions*

QUESTION ONE (30 MARKS)

a) i) Define the greatest common divisor (GCD) of a and b where a and b are integers (3 marks)

ii) Using division algorithm find the least common multiple of $a = 2464$ and $b = 7469$ (6 marks)

b) i) If $a, b, c \in \mathbb{Z}$ and $a|b$ and $b|c$ prove that $a|c$ (3 marks)

ii) If $a|b$ ab and $a|c$ a/c and m and n are integers, then $a|(mb+nc)$ (3 marks)

c) Given that a and b are integers then $ab = (a,b)[a,b]$. Prove (5 marks)

QUESTION TWO (20 MARKS)

a) i. Define a prime number (2 marks)

ii. Prove by contradiction that there is an infinity of prime numbers (5 marks)

b) i. Define a composite number (2 marks)

ii. If n is composite, explain why n must have a prime factor $p \leq \sqrt{n}$ (3 marks)

iii. Write the numbers from 2 to 100 then cross out all proper multiples of 2 and continue with all proper multiples of $3,5,7,\left(\angle\sqrt{100}\right)$ to find all prime numbers less than 100

(5 marks)

c) Show that there are infinitely many primes of the form $6n-1$ where $n\epsilon\mathbb{N}$ (3 marks)

QUESTION THREE (20 MARKS)

a) Explain the meaning of "a is congruent to b module m" (3 marks)

b) Show that $a \equiv b(\text{mod}\, m)$ is an equivalence relation on $\mathbb{Z}$ (3 marks)

c) i. Let $\cap\, \epsilon\mathbb{N}$ and write $\cap = a_0 + 10a_1 + 10^2a_2 + \cdots 10^k a_k$ Show that 9/n

(4 marks)

ii. Using fast powering algorithm compute $5^5 (\text{mod}\, II)$ (4 marks)

d) State and prove Fermat's "little" theorem (6 marks)

QUESTION FOUR (20 MARKS)

a) Let p, q be decisional primes, $a\epsilon\mathbb{Z}$,and $\left(k^1, (p-1)(q-1)\right) = 1$. Take e to be an inverse of k mod the $lcm[p-1, q-1]$. Show that $x = a^e (\text{mod}\, pq)$ is a solution to $x^k \equiv a(\text{mod}\, p\varepsilon)$ (4 marks)

b) Describe the RSA algorithm using

i. (S = Sender, R = Receiver) (6 marks)

ii. Using $p = 17,\ q = 19,$ verify the above RSA algorithm (6 marks)

c) Differentiate between symmetric and asymmetric cipers (4 marks)

QUESTION FIVE (20 MARKS)

a) Describe elliptic El Gamal cryptosystem basic algorithm (4 marks)

b) Let $P = 1123, E : y^2 = x^3 + 54x + 87$ and suppose we are sent the "point of $E(Fp)$" $x_0 = 278, \beta_o = 0$. Find y_0 (5 marks)

c) Explain the discrete log problem

i. (DLP) in public key cryptography (5 marks)

ii. An eaves dropper E sees p, g, g^{α} *and* g^{β}. In order to find $g^{\alpha\beta}; s$ he would have to compute log(g^{α}) or log (g^{β}) using $P = 11,$ and $g = z$ is a generator and Alice (sender) chooses $\alpha = 6,$ find what he sends to Bob(receiver). If Bob choose $\beta = 7$ and sends to Alice, find what she receives. Find also the shared secret s (6 marks)