JARAMOGI OGINGA ODINGA UNIVERSITY

OF SCIENCE & TECHNOLOGY

UNIVERSITY EXAMINATIONS 2012/2013

2ND YEAR 1ST SEMESTER EXAMINATION FOR THE DEGREE OF BACHELOR OF SCIENCE (COMPUTER SECURITY AND AUDIT)

(KISUMU L.CENTRE)

COURSE CODE: IIT 3218

COURSE TITLE: INTRODUCTION TO NUMBER THEORY

DATE: 15/8/2013 **TIME: 2.00-4.00 PM**

DURATION: 2 HOURS

INSTRUCTIONS

1. **This paper consists of 5 Questions.**
2. **Answer Question 1 (Compulsory) and any other 2 questions.**
3. **All workings must be shown clearly.**
4. **Write your answers on the answer booklet provided.**

QUESTION ONE (30 marks)

a) Give a precise definition of a prime number P. [2 Marks]

b) What are the prime factorizations of the following numbers:
$100,\ 641$ and 999. [3 Marks]

c) Find the quotient q and the remainder r whenit is divided by 3 [2 Marks]

d) Find the base 8 expansion of $(341675)_{10}$. [5 Marks]

e) Add $a=(1110)_2$ and $b=(1011)_2$. [4 Marks]

f) How many divisions are required to find $\gcd(34,55)$ using the Euclidean algorithm? Explain your answer. [5 Marks]

g) Find the product of $a=(110)_2$ and $b=(101)_2$. [4 Marks]

h) Given the algorithm below:

ALGORITHM 1 Multiply Integers
procedure multiply (a, b: positive integers)
{the binary expansions of a and b are $(a_{n-1}\ a_{n-2}\ \ldots a_1\ a_0)_2$
and $(b_{n-1}\ b_{n-2}\ \ldots\ b_1\ b_0)_2$ respectively }
for j:=0 **to** n-1
begin
if b_j=1 **then** c_j:=a shifted j places
else c_j:=0
end
{c_0,c_1 ,…,c_{n-1} are the partial products}
P:=0
for j:=0 **to** n-1
p:= p+c_j
{p is the value of ab}

How many additions of bits and shifts of bits are used to multiply a and b using Algorithm1 above? [5 Marks]

QUESTION TWO (20 marks)

a) Generate a sequence of pseudorandom numbers $\{x_n\}$, with $0 \le x_n \le m$ for all n using the congruence

$$x_{n+1} = (ax_n + c) \bmod m$$

given that $m = 7,\ a = 5, c = 4$ and $x_0 = 3$. [8 Marks]

b) Let m be a positive integer. If $a = b \pmod m$ and $c = d \pmod m$, prove that $a + c = b + d \pmod m$. [7 Marks]

c) Find an inverse of 3 modulo 7. [5 Marks]

QUESTION THREE (20 marks)

a) Distinguish between the integers being relatively prime and pairwise relatively prime and hence determine whether the integers 10, 19 and 24 are pairwise relatively prime. [6 Marks]

b) Find prime factorization of 77077. [7 Marks]

c) Let m be a positive integer. Prove that the integers a and b congruent modulo m if and only if there is an integer k such that $a = b + km$. [7 Marks]

QUESTION FOUR (20 marks)

a) The packing lot for a local restaurant has 41 parking spaces, numbered consecutively from 0 to 40. A parking attendant at the restaurant uses the hashing function $h(k) = k \bmod 41$, where k is the integer obtained from the three digits on the patron's number plate, to give a parking lot. Suppose that 8 cars arrive as the restaurant opens. If their number plates (in order of arrival) are: 206, 807, 137, 444, 617, 330, 465, 905 respectively. Which places are assigned to these patrons by the parking attendant? [15 Marks]

b) Encrypt the message

DO NOT WAIT ANYMORE

Using Caersar's Cipher. [5 Marks]

QUESTION FIVE (20 marks)

a) Use the encryption key: $E(x)=(x+7)$ **mod** 26

To decrypt the following coded message sent by a student to his parents:

Z L U K T V Y L T V U L F [7 Marks]

b) Using the affine Cipher, where;

$E(\theta)=(11\theta+7)$ **mod** 26

Find which letter represents the plaintext letter G
in the encrypt Cipher text. [7 Marks]

c) Let $a = bq + r$, where a, b, q and r are integers. Show that $\gcd(a,b) = \gcd(b,r)$. [6 Marks]