**KIBABII UNIVERSITY COLLEGE**
*(A Constituent College of MasindeMuliro University of Science Technology)*
P.O. Box 1699-50200 Bungoma, Kenya
Tel. 020-2028660/0708-085934/0734-831729
E-mail: enquiries@kibabiiuniversity.ac.ke

**UNIVERSITY REGULAR EXAMINATIONS**

**2013/2014 ACADEMIC YEAR**

**MAIN EXAMINATION**

**DEPARTMENT OF COMPUTER SCIENCE**

**COURSE CODE: CSC 372**

**COURSETITLE: APPLIED CRYPTOGRAPHY**

**DATE: 15TH APRIL, 2014** **TIME: 2:00A.M. – 5:00P.M.**

***Instructions: Answer all the questions in section I and any two in section II***

## Section I (30 Marks)

## QUESTION ONE (30 MARKS)

a) Write short notes on

i. Public-key encryption

ii. Digital Signatures

iii. Brute force attack(6mks)

b) Consider a substitution cipher where 52 symbols were used instead of 26. In particular, each symbol in the cipher text is for either a lowercase English letter, or an uppercase English letter. Does this provide added security compared to a standard substitution cipher (3 mks)

c) John have found one small piece of matching plaintext and ciphertext for a Hill cipher using a 2x2 matrix key with mod 17 entries. In particular, the plaintext (12, 5) maps to the ciphertext (14, 10). List two of these possible keys. (6 mks)

d)What are the two basic functions used in an encryption algorithm (2 marks)

e) Briefly define the monoalphabetic cipher (3 marks)

f) Construct a play fair matrix with the key LARGEST (5 mks)

g) Encrypt the message “meet me at the usual place at ten rather than eight oclock” using a hill cipher with the key $\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$. show your calculations. (5 mks)

## Section II (40 MARKS)

## QUESTION TWO (20 MARKS)

a)i) Let $X'$be the bitwise complement of $X$. Prove that if the complement of the plaintext block is taken and the complement of an encryption key is taken, then the result of DES encryption with these values is the complement of the original cipher text. That is if

$$Y = E(K, X)$$

Then $Y' = E(K', X')$ (5 mks)

ii) A brute-force attack on DES requires searching a key space of $2^5$ keys. Does the result of (i) above change that (5 mks)

b) Show that DES decryption is the inverse of DES encryption (10 mks)

**QUESTION THREE (20 MARKS)**

a) Compute the bits numbers 1, 16, 33 and 48 at the output of the first round of the DES decryption assuming that the cipher text block is composed of all ones and the external key is composed of all ones. (10 marks)

b) Let R be the ring defined by polynomials with coefficients in $Z_2$ with all computations reduced modulo $x^6+1$. Prove that R has:

i) Multiplicative Identity
ii) No zero divisors
iii) Multiplicative Inverse (5 marks)

c) Find $3^2$ $m$ 11 using Fermat's theorem (5 marks)

**QUESTION FOUR (20 MARKS)**

a) Six professors begin courses on Monday, Tuesday, Wednesday, Thursday, Friday and Saturday respectively and announce their intentions of lecturing at intervals of 2,3,4,6 and 5 respectively. The regulation of the university forbids Sunday lectures. When first will all six professors find themselves compelled to omit a lecture. (8 mks)

b) Find all primitive roots of 25 (3 mks)

c) For$E_1$ (1,6), consider the point $G$(2,7). Compute the multiples of G from 2G and 13G. (7mks)

d) What are the two general approaches to attacking a cipher (2mks)

**QUESTION FIVE (20 MARKS)**

a) A cipher text has been generated by an affine cipher. The most frequent letter of the ciphertext is ‘B’ and the second most frequent letter of the ciphertext is ‘U’. Break this code. (5 mks)

b) List and briefly define three classes of intruders (6 mks)

c) Suppose that in PCBC mode, blocks $c_i$ and $c_{i+1}$are interchanged during transmission. Show that this affects only the decrypted blocks $p_i$ and $p_{i+1}$but not subsequent blocks. (9 mks)