(K*nowledge for Development)*

KIBABII UNIVERSITY COLLEGE

A CONSTITUENT COLLEGE OF

MASINDE MULIRO UNIVERSITY OF

SCIENCE AND TECHNOLOGY

UNIVERSITY EXAMINATIONS

2014/2015 ACADEMIC YEAR

THIRD YEAR SECOND SEMESTER

MAIN EXAMINATION

FOR THE DEGREE OF

BACHELOR OF SCIENCE COMPUTER SCIENCE

COURSE CODE: CSC 372 E

COURSE TITLE: APPLIED CRYPTOGRAPHY

DATE: 7TH MAY, 2015 **TIME:** 11.30-1.30PM

INSTRUCTIONS TO CANDIDATES

Answer Question One in Section A and Any other TWO (2) Questions in Section B

TIME : 2 HOUR

Question One (30 Marks)

a) List and briefly define categories of security services (5 Marks)
b) Compute the bits number 1, 16, 33 and 48 at the output of the first round of the DES decryption, assuming that the ciphertext block is composed of all ones and the external key is composed of all ones. (3.6) (6 Marks)
c) Determine the gcd(24140,16762) (4.1..) (4 Marks)
d) Using Fermat's theorem, find 3^{2} m 11. (8.3) (3 Marks)
e) In a public-key system using RSA, you intercept the ciphertext $C = 10$ sent to a user whose public key is $e = 5, n = 35$. What is the plaintext M? (9.3) (4 Marks)
f) Find the multiplicative inverse of each nonzero element in $\mathbb{Z}_5$(4.14) (4 Marks)
g) Construct a playfair matrix with the key *largest*.(2.10) (4 Marks)

Question Two (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 Marks)

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

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 Marks)

Question Three (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 Marks)

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

c) ForE_1 (1,6), consider the point $G(2,7)$. Compute the multiples of G from 2G and 13G. (7 Marks)

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

Question Four (20 Marks)

a) 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. (8 Marks)

b) What are the two basic functions used in an encryption algorithm (2 Marks)

c) Briefly define the monoalphabetic cipher (2 Marks)

e) 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. (8 Marks)

Question Five (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 Marks)

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 Marks)

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