Mid-West University

Examinations Management Office

End Semester Examinations -2080

Bachelor level/ B.Sc CSIT / 6th Semester — Full Marks: 60

Time: 3 hours — Pass Marks: 30

Subject: Cryptography (COM464)

Candidates are required to give their answer in their own words as far as practicable. The figures in the margin indicate full marks.

Group A

Long Answer Questions (Any Three) **[3x8=24]**

1) Explain about DES, 3DES and AES in details.
2) What is electronic codebook? Explain about IDEA & MD5.
3) What is MD5? Explain Diffie-Hellman Key-Exchange algorithm.
4) a) Make a cipher text of the plain text **TRUE** where key is **graduate school** by using **HILL** cipher substitution.

   b) Make the Caesar Cipher text of the Plain text: **MID WEST UNIVERSITY**. (Use C= (P+3) mod 26)

Group B

Short Answer Questions (Any Five) **[5x4=20]**

5) What are the security threats and attack? Explain shortly.
6) Compare block cipher with stream cipher in at least 6 parameters.
7) Make a cipher text **orange** having key **snow** with the help of **Vigenere** cipher.
8) What do you mean by substitution cipher? Explain Hash Function and their application.
9) What is biometric authentication? Explain RSA algorithm.
10) How message authentication is carried out using Encryption?

Group C

Very Short Answer Questions **[8x2=16]**

11) How can you relate encryption and decryption?
12) List out the symmetric and asymmetric ciphers.
13) Define cryptology and steganography.
14) What is number theory and how it is used in cryptography?
15) What is confidentiality, Integrity & Authentication?
16) What is Elliptic curve cryptography?
17) How digital signature is differing from DSS?
18) What is malicious logic, Virus, Worm & Intruders?

THE END