Mid-West University

Examinations Management Office

End Semester Examinations 2081

Bachelor level/ B.Sc. /CSIT 6th Semester
Time: 3 hours
Subject: Cryptography (COM464)

Full Marks: 60
Pass Marks: 30

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

Very short answer questions. Attempt all the questions. **[8x2 = 16]**

1. How can you relate computer security and information security?
2. What is OSI security architecture?
3. Define cryptology and cryptoanalysis.
4. What is elgamal cryptosystem? How it is used in cryptography?
5. What is confidentiality, Integrity & Availability?
6. What is electronic codebook?
7. How digital signature is used in message authentication?
8. What do you mean by Public Key Cryptography?

Group B

Short answer questions. Attempt *any five* questions. **[5x4 = 20]**

9. What are the security services and mechanism? Explain shortly.
10. Compare block cipher with stream cipher in at least 6 parameters.
11. Make a cipher text **banana** having key **yellow** with the help of **Vigenere** cipher.
12. What do you mean by transposition cipher? Explain Hash Function and their application.
13. Differentiate between Block Cipher and Stream Ciphers. Explain RSA algorithm.
14. How message authentication is carried out using SHA?

Group C

Long answer questions. Attempt *any three* questions. **[3x8 = 24]**

15. Discuss about DES, 3DES and AES in details.
16. What is elliptic curve cryptography? Explain about IDEA & MD5.
17. What is RC4? Explain Diffie-Hellman Key-Exchange algorithm.
18. (A) Make a cipher text of the plain text **NOTE** where key is **graduate school** by using **HILL** cipher substitution.

    (B) Make the Caesar Cipher text of the Plain text: **COMPUTER SCIENCE.** (Use C= (P+3) mod 26

The End