

Mid-West University  
**Examinations Management Office**  
**Surkhet, Nepal**  
Final Examinations -2079

Bachelor level/ B.Sc. CSIT /6th Semester  
Time: 3hrs  
**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 Questions Answer (Attempt all)**

[8x2=16]

1. Define cryptography.
2. Point out the technique to secure the information.
3. Write the steps to Steganography.
4. Define state array.
5. Write about the primality testing.
6. Calculate the mode value of  $2^{644}$  mode 645.
7. How virus is different from worms?
8. Write short notes on prime and coprime number.

**Group B**

**Short Questions Answer (Attempt any five)**

[5x4=20]

9. Illustrate the OSI Security Architecture.
10. Write about the various types of Data Encryption Standards (DES) .
11. Define Blocked cypher. Mention its benefits and limitations.
12. What is Elgamal cryptosystem? Describe its process.
13. What is digital signature? Explain its techniques.
14. Explain online and offline dictionary attack.

**Group C**

**Long Questions Answer (Attempt any three)**

[3x8=24]

15. Explain the types of cryptography with illustration.
16. Describe RSA algorithm for encrypt and decrypt the message with example.
17. Describe Euler Totient function. Explain various properties of Euler totient function with illustration.
18. What is authentication in cryptography? Explain the password based authentication and biometric authentication technique.

**THE END**