B. R. A. BIHAR UNIVERSITY
MUZAFFARPUR
MODEL -Q- OF MCA COURSE
(CS 402: `Cryptography & Network Security`)

1. Explain about OSI Security Architecture ?
   'or'
   Explain the Security Mechanism and describe X.800?
2. Explain simplified data encryption standard with example with example.
3. (ea) State the format's theorem.

4. What are the services provided by if security?
   Describe the architecture of IP security.
5. Explain the Chinese Reminder Theorem (CRT). Find the value of
   X for the congruence equations.
   $X \equiv 2 \bmod 7$ and $2 \equiv 3 \bmod 9$
6. Briefly explain the Design Principles of block cipher.
7. What is massage Authentication? Specify the requirements for massage authentication?
8. Explain the four protocol define by search socket layer.
9. What is the need for security services at transport layer of internet protocol.
10. Explain RSA Algorithm with an example.
11. Explain in detail:| about blowfish.
12. Draw the general structure of AES algorithm. Explain how Encryption and Decryption are carried out using AES. What is the strength of this algorithm?
13. (a) Discuss various cryptographic a hacks.
    (b) Describe Cipher chipper and mono alphabetic cipher with suitable examples.
14. (a) How signing and verification is done in digital signature algorithm?
    (b) Discuss about the various types of firewall.
15. Discuss on the significant types of various categories.
16. Explain about RC-4 algorithm.
17. Describe about SSL/TLS protocol.