CELEBRATING 25 YEARS
CMRIT
CMR INSTITUTE OF TECHNOLOGY, BENGALURU.
ACCREDITED WITH A+ GRADE BY NAAC
No.132, AECS Layout
I.T. Park Road, Bangalore 560 037
T: +91 80 28524466/77, F : +91 80 28524630
E: info@cmr.ac.in I www.cmr.ac.in

DEPARTMENT OF INFORMATION SCIENCE & ENGINEERING

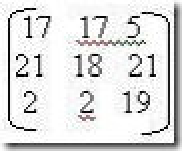
CRYPTOGRAPHY, NETWORK SECURITY AND CYBER LAW [17CS61] -QUESTION BANK

Faculty: Bineet Kumar Jha

Module 1

1. Enumerate common attacks and vulnerabilities.
2. Interpret defense strategies and techniques
3. Explain Chinese Remainder theorem.
4. Describe in brief about mono alphabetic cipher.
5. Describe in brief about polyalphabetic cipher.
6. Explain in detail Transposition Technique.
7. Convert the plaintext Welcome to cryptography into cipher text using Transposition Technique.
8. Convert the plaintext Welcome to cryptography into cipher text using Vigenere cipher and key as NETWORK.

9. Convert “MEET ME” using Hill cipher with the key matrix



$$\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$$

Convert the cipher text back to plaintext

10. Illustrate DES construction.

Module 2

1. Perform decryption and encryption using RSA algorithm with p=3, q=11, e=7 and M=5.
2. Identify the practical issues in implementing RSA algorithm
3. Explain public key cryptography standard.
4. Enumerate SHA1

5. Illustrate Digital Signature
6. Interpret HMAC
7. Explain in brief about Diffie Hellman key exchange
8. Explain about Elgamal encryption

Module 3

1. Enumerate public key infrastructure
2. Explain one way authentication
3. Explain mutual authentication
4. Discuss about dictionary attacks
5. Illustrate Needham-Schroeder protocol
6. Briefly explain about Kerberos.
7. Interpret Biometrics.
8. Explain IP security.
9. Brief about Internet key exchange protocol.
10. Explain SSL handshake protocol.

Module 4

1. Explain about confidentiality and integrity.
2. Explain about authentication.
3. Enumerate virus, worms and other malware.
4. Briefly explain about firewalls.
5. Elaborate Intrusion Detection and prevention system with its types.
6. Elaborate DDoS attack Detection and prevention system.
7. Explain about web service security.
8. Illustrate SAML.

Module 5

1. Explain IT act and objectives
2. Brief about important provisions.
3. Enumerate about electronic records and secure digital signatures.
4. Explain regulation of certifying authorities.
5. Describe digital signature certificates.
6. Explain the duties of subscribers.
7. Explain the cyber regulations appellate tribunal.
8. Illustrate miscellaneous provisions.