Priyadarshini College of Engineering, Nagpur

Department of Computer Technology

Session 23-24

CNS Tutorial

Subject : Cryptography and Network Security

Semester : VII A/B

Subject Teachers : Mr. P.U. Tembhare / Mrs.Snehal Bhujade

Unit : I,II, III , IV, and V

Tutorial No.	Tutorial Questions
1	a) Explain additive cipher ? Use additive cipher with key=2 to encrypt message " **COMPUTER**" b) Using the key "**COMPUTER**" encrypt the message "**Transfer**" by using Vigenere cipher. (CO1)
2	Explain the substitution Techniques? If the cipher is keyed by a word "**COMPUTER**" and Plaintext is "**Please transfer one million dollars to my account six six two"** obtain the cipher text by Playfair Substitution Methods? (CO1)
3	a) Explain DES in detail b) Difference between : Private vs Public key cryptography **(CO2)**
4	a) Explain a AES algorithm? How is different from DES algorithm? in details. b) Explain a block cipher principles? What is difference between stream ciphers and block cipher? **(CO2)**
5	Write RSA Algorithm? Perform Encryption using the RSA Algorithm, for the following. P=7, q=11, e=3, M=9
6	chines problem
7	write a note on : ECC
8	Explain Has function
9	Describe Diffie - Hellman key exchange algorithm.

10	Solve modular expontial algorithm : 1)23 power 3 mod 30 2)11 power 23 mod 187
11	Explain the following terms- i) Trap doors and cross site scripting. ii) Host based v/s Network based IDS
12	Short Note on any three. a) PGP b) SQL injection. d) Chip Card Transaction.

Mr. P.U. Tembhare / Mrs.Snehal Bhujade
(Subject Teachers)

Dr. (Mrs.) N. M. Thakare
(HOD, CT)