

VEER SURENDRA SAI UNIVERSITY OF TECHNOLOGY, BURLA
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
& INFORMATION TECHNOLOGY
SESSION 2014-2015 (EVEN SEMESTER)

Total Pages—3

(Set-1)

B.Tech-8th

Cryptography & Network Security

Full Marks : 70

Time : 3 hours

Answer Q. No. 1 which is compulsory and
any five from the rest

The figures in the right-hand margin indicate marks

- I. Answer the following questions : 2 × 10
- (a) What do you mean by sniffing and spoofing ?
 - (b) What is the difference between worm and virus ?
 - (c) What is the main feature of polygram substitution cipher ?
 - (d) What is Rail-Fence technique ? Explain with example.
 - (e) What is an Initialization vector (IV) ? What is its significance ?

(Turn Over)

(2)

- (f) What is the idea behind meet-in-the-middle attack? 5
- (g) Describe the advantages and disadvantages of symmetric and asymmetric key cryptography. 5
- (h) What is the difference between MAC and Message digest. 5
- (i) What are the common causes for revoking a digital certificate? 5
- (j) What is the security concern in WAP? 5
2. (a) Use a Hill cipher to encipher the message "We do not live in secure world". 5
- $$K = \begin{bmatrix} 3 & 2 \\ 5 & 7 \end{bmatrix}$$
- (b) What is the difference between transposition cipher and substitution cipher? Explain with suitable example. 5
3. (a) Explain AES cryptosystem in brief. 5
- (b) Explain RC5 in details. 5

(3)

4. (a) Explain the RSA cryptosystem. 5
- (b) In RSA, given $e = 13$ and $n = 100$ encrypt the message "Computer" using 00 to 25 for letters A to Z and 26 for the space. 5
5. (a) Explain Knapsack Algorithm. 5
- (b) Explain ElGamal cryptosystem based on digital signature. 5
6. (a) What do you mean by digital certificate? Write down the steps how digital certificate created. 5
- (b) Discuss password based Encryption in brief. 5
7. (a) Explain 3-D secure protocol. 5
- (b) Explain briefly about E-mail security. 5
8. Write short notes on : 5+5
- (i) WAP security
- (ii) Security in GSM.