F – 2949

(Pages : 2)

Reg. No. : .....

Name : .....

Eighth Semester B.Tech. Degree Examination, December 2018
(2013 Scheme)
13.801 : Cryptography and Network Security (R)

Time : 3 Hours Max. Marks : 100

PART – A

Answer **all** questions, **each** question carries **four** marks.

1. Use an affine cipher to decrypt the message "ZEBBW" with the key pair (7, 2) in modulus 26.
2. What is the structure of each round in AES encryption ?
3. Use Fermat's little theorem to find 7^{222} mod 11.
4. What is format of a PGP packet header ?
5. What are the different types of firewalls ?

PART – B

Answer **any one full** question from **each** Module.

Module – I

6. a) Using the Vigenère cipher, encrypt the word "explanation" using the key LEG. 5

   b) Explain about the components used in DES function. 15

OR

7. a) Using the following playfair matrix, encrypt the message: I AM A COOL PERSON. 5

M	F	H	K	I/J
U	N	O	P	Q
Z	V	W	X	Y
E	L	A	R	G
D	S	T	B	C

P.T.O.

b) Explain the general design of AES encryption cipher. **12**

c) Analyze the three characteristics of AES. **3**

Module – II

8. a) What are the steps for Diffie-Hellman key agreement ? **10**

b) What are the three properties for hash function which is used in cryptographic algorithms ? **5**

c) Differentiate between MAC and digital signature. **5**

OR

9. a) Elaborate RSA cryptosystem. **10**

b) Compute Secret key, d and Ciphertext, C by using RSA algorithm where $p = 5, q = 11, e = 3, M = 9$. **5**

c) Prove that RSA is not Chosen Ciphertext Attack (CCA) secure. **5**

Module – III

10. a) What are different modes of IPSec operation ? **5**

b) Explain IPSec protocols with the help of diagrams. **15**

OR

11. a) Explain about Cryptographic Message Syntax (CMS) which is defined in S/MIME. **10**

b) Define Kerberos and explain the key management with the help of its servers. **10**

Module – IV

12. a) Differentiate between session and connection. **10**

b) Explain about the generation of cryptographic secrets in TLS. **10**

OR

13. Explain about four protocols used in SSL. **(4×5=20 Marks)**