Register Number:…………….

M.E DEGREE EXAMINATIONS: DEC 2015

(Regulation 2014)

Third Semester

COMMUNICATION SYSTEMS

P14COTE22: Communication Network Security

Time: Three Hours **Maximum Marks: 100**

Answer all the Questions:-

PART A (10 x 1 = 10 Marks)

1. The Caesar cipher involves replacing each letter of the alphabet with letter standing CO1 [K_2]

a) Four places b) Two places

c) One place d) Three places

2. A stream cipher is one that encrypts a digital data stream CO1 [K_2]

a) Two bits or two bytes at a time b) One bit or one byte at a time

c) One bit or two bytes at a time d) Two bits or one byte at a time

3. Virtually all encryption algorithms both conventional and public key involve CO1 [K_2]

a) Arithmetic operations on integers b) Italic operations on integers

c) Alphanumeric operations on integers d) Boolean operations on integers

4. Match list I with list II and select the correct answer using the codes given CO1 [K_4]

List I	**List II**
A. pseudo random generator	i. $C = E(K_2, E(K_1,P))$
B. Double DES	ii. triple encryption
C. Tuchman	iii. stream cipher
D.RC4	iv. Deterministic algorithm

	A	B	C	D
a)	iv	i	ii	iii
b)	iii	i	ii	iv
c)	iii	ii	iv	i
d)	i	ii	iii	iv

5. Assertion (A):The concept of public key cryptography evolved from an attempt to attack the most difficult problems associated with symmetric encryption the first CO2 [K_3]

problem is key distribution and second digital signatures

Reason (R):key distribution and digital signatures are difficult problems

a) Both A and R are individually true and R is the correct explanation for A
b) A is true but R is false
c) Both A and R individually true but R is not correct explanation of A
d) A is false but R is true

6. Discrete logarithm is stated as CO2 [K_2]

a) $y = x^{\log y}$
b) $y = g^x$ And p
c) $y = g^x \bmod p$
d) $y = g^x$ xor p

7. Authentication consists of CO3 [K_2]

a) Identification only
b) Identification step and verification step
c) Verification step only
d) Identification step authentication step and ticket granting step

8. Secure socket layer protocol is a CO4 [K_2]

a) One layer protocol
b) Two layer protocol
c) Three layer protocol
d) Four layer protocol

9. Intruder is a individual who is CO4 [K_2]

a) Friendly user
b) Genuine user
c) Authorized user
d) Clandestine user

10. Consider the following statements. CO5 [K_4]

1. Cisco is router manufacturing company
2. 3com is a computer networking company
3. Texas instruments is a computer networking company
4. Analog devices is a computer networking company.

Which of these statements are correct

a) 1,2
b) 1,3
c) 3,4
d) 2,3

PART B (10 x 2 = 20 Marks)

11. Compare Caesar cipher and monoalphabetic ciphers. CO1 [K_2]

12. Distinguish between Feistel decryption and DES decryption. CO1 [K_4]

13. Summarize the stream cipher structure. COL [K_2]

14. Distinguish between link and End –to –End Encryption. CO1 [K_4]

15. Compare linear congruential generators and blum blum shrub random number generators. CO2 [K_2]

16. Select a suitable Hash algorithm for security stating the reasons CO3 [K_5]
i)SHA-1 ii)SHA-256 iii)SHA-384 iv)SHA-512.

17. Compare Kerberos Version 4 and Kerberos version 5 the authentication service. CO3 [K_2]

18. Summarize the features of authentication header. CO3 [K_2]

19. Distinguish between Worm and Virus. CO5 [K_4]

20. Select a suitable advanced Antivirus technique from the three approaches stating reasons CO5 [K_4]
i)Generic Decryption ii)Digital immune system iii)Behavior blocking software

PART C (10 x 5 = 50 Marks)

21. Summarize the features of security mechanisms. CO1 [K_2]

22. Explain stegnography used in plaintext hiding. CO1 [K_2]

23. Evaluate the criteria for AES. CO2 [K_2]

24. Analyze Triple DES with two keys and obtain expression for the expected running time of attack. CO2 [K_4]

25. Summarize the elliptic curve arithmetic used in public key encryption. CO3 [K_2]

26. Analyze and obtain expressions digital signature standards signing and verifying. CO3 [K_4]

27. Explain SSL architecture and its connection state parameters. CO4 [K_2]

28. Explain the overview of secure electronic transaction. CO4 [K_2]

29. Explain the various firewall characteristics. CO5 [K_2]

30. With a table explain terminology of malicious programs. CO5 [K_2]

PART D (2 x 10 = 20 Marks)

31. i)Design the logic of a general block substitution cipher for n=4.A 4bit input producing one of 16 possible input states which is mapped by the substitution cipher into a unique 16 possible output states each of which is represented by 4 cipher text bits. Also give an illustration figure. 6 CO1 [K_4]

ii)Explain the overall scheme of DES encryption 4 CO1 [K_2]

32. i) Explain the following terms of Pass word Management 5 CO5 $[K_2]$

Password protection ,the vulnerability of passwords, password selection strategies

ii) Compare the various types of Viruses. 5 CO5 $[K_2]$

****