KUMARAGURU
college of technology
character is life

Register Number:……..…

M.E. DEGREE EXAMINATIONS: JUNE 2016

(Regulation 2015)

Second Semester

COMMUNICATION SYSTEMS

P15COTE10: Communication Network Security

COURSE OUTCOMES

CO1: Classify the symmetric encryption techniques.

CO2: Illustrate various Public key cryptographic techniques.

CO3: Evaluate the authentication and hash algorithms

CO4: Elaborate the network security and web security techniques

CO5: Identify intrusion detection and its solutions to overcome the attacks.

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

Answer all the Questions:-

PART A (10 x 1 = 10 Marks)

1. The Cipher text for the message “hard work never fails” using Caesar cipher is CO1 [K_2]

   a) MFWI BTWP SJAJW KFNQX b) LEVH ASVO RIZIV JEMPW

   c) KDUG ZRUN QHYHU IDLOV d) JCTF YQTM PGXGT HCKNU

2. The disadvantages on one time pad are CO1 [K_1]

   1. Making large quantities of random keys
   2. Requirement of lot of overhead
   3. Key distribution and protection
   4. All knowledge of the plain text structure is lost
   5. Identification of individual digrams is difficult

   a) 2,4,5 b) 1,3

   c) 1,3,5 d) 2,3

3. A covert channel is CO1 [K_2]

   a) Unintended by the designers of the communication facility b) Correlating the conversations between particular partners.

   c) Non-violation of security policy d) Improper identity of partners

4. Match the following: CO1 [K_2]

List I	List II
A. Key size	i. 128
B. Expanded key size	ii. 10/12/14
C. Rounds	iii. 128/192/256
D. Round key size	iv. 176/208/240

a) iv, iii, i, ii.
b) i, ii, iii, iv.
c) iii, iv, ii, i.
d) i, ii, iv, iii.

5. Choose the sequence of steps involved in the following process. CO2 [K_2]

The steps to perform RSA algorithm is as follows

1. Determine d such that de = 1mod □(n)
2. Select two prime numbers p and q
3. Select e such that e is relatively prime to ≤ □(n)
4. Calculate □(n) = (p-1)(q-1)
5. Calculate n = pq

a) 2, 5, 4, 1, 3
b) 2, 4, 5, 3, 1
c) 2, 4, 5, 1, 3
d) 2, 5, 4, 3, 1

6. The reason for the acceptance of hybrid scheme to distribute secret keys in public key encryption is its CO2 [K_2]

a) performance
b) Backward compatibility
c) Performance and backward compatibility
d) Confidentiality, authentication and compatibility.

7. Assertion (A): RC4 has variable key size and byte oriented operations CO1 [K_3]

Reason (R): RC4 is widely used stream cipher

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

8. The strength of hash function against brute-force attacks depends on CO3 [K_2]

a) One way function
b) Generation of independent subcodes
c) Encrypted hash code
d) Length of the hash code produced by the algorithm

9. The reason for the growth of PGP is CO4 [K_2]

1. Run on variety of platforms

2. Internet standards track
3. Wide range of applicability
4. It is developed and controlled by governmental organizations

a) 1 and 2 are true
b) 1,2 and 3 are true
c) All the statements are true
d) Only the statement 4 is true.

10. The virus that creates copies during replication that are functionally equivalent but have distinctly different bit patterns. CO5 [K_1]

a) Polymorphic virus
b) Stealth virus
c) Parasitic virus
d) Memory resident virus

PART B (10 x 2 = 20 Marks)

11. Distinguish between diffusion and confusion. CO1 [K_2]
12. Compare Differential and linear cryptanalysis. CO1 [K_2]
13. What is a trap-door one way function? CO2 [K_2]
14. What is a public-key certificate? CO2 [K_3]
15. What changes in HMAC are required in order to replace one underlying hash function with another? CO3 [K_2]
16. What are the basic arithmetical and logical functions used in SHA -1? CO3 [K_2]
17. What problem was Kerberos designed to address? CO4 [K_2]
18. Compare the functionalities of Transport and tunnel mode of IP security. CO4 [K_2]
19. What are the basic techniques of choosing password? CO5 [K_2]
20. What is a digital immune system? CO5 [K_2]

PART C (6 x 5 = 30 Marks)

21. Encrypt the plain text “Hard Work” using Hill cipher technique with the key $\begin{pmatrix} 7 & 8 \\ 19 & 3 \end{pmatrix}$ CO1 [K_3]

22. In Diffie-Helman Key Exchange, q = 71 and its primitive root α = 7. A’s private key is 5, B’s private key is 12. Find (i) A’s public key (ii) B’s Public key and (iii) Shared secret key. CO2 [K_3]

23. Describe briefly the Digital signature technique and its requirements CO3 [K_2]

24. Explain X.509 Authentication service and its procedure. CO4 [K_2]

25.	On Elliptic Curve $E_{11}(1,6)$, consider the points G = (2,7) and H = (4,3). Compute 2G and G+H.	CO3	[K_3]
26.	Discuss on the capabilities and limitations of firewalls.	CO5	[K_2]

Answer any FOUR Questions

PART D (4 x 10 = 40 Marks)

27.	With the schematic diagram, explain the S-DES encryption and decryption process. Highlight the key generation phase for the plain text 10101100 with the key 10000100110 if P_{10} = 3 5 2 7 4 10 1 9 8 6 and P_8 = 6 3 7 4 8 5 10 9.	CO1	[K_4]
28.	Discuss briefly the block cipher modes of operation. Compare and contrast the advantages and disadvantages of them.	CO1	[K_3]
29.	List the classification of Authentication functions and explain each in detail.	CO3	[K_2]
30.	Explain the various phases of SSL handshake protocol.	CO4	[K_2]
31.	Explain the architecture of Distributed Intrusion Detection with diagram and give examples of metrics useful for profile based intrusion detection.	CO5	[K_2]

****