Register Number:……..

KUMARAGURU college of technology
character is life

B.TECH DEGREE EXAMINATIONS: MAY 2017

(Regulation 2014)

Sixth Semester

INFORMATION TECHNOLOGY

U14ITT603: Cryptography and Network Security

COURSE OUTCOMES

CO1: Explain security attacks and issues in computer systems and networks.
CO2: Explain the mathematics behind Cryptography
CO3: Explain the purpose and working of various algorithms related to cryptography, authentication, network security and system security algorithms.
CO4: Identify the appropriate security mechanism for different computing environment and information systems.
CO5: Apply appropriate security methods to solve real life applications.

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

Answer all the Questions:-

PART A (10 x 1 = 10 Marks)

1. CO1 [K_2]

List I	List II
A. Rail fence technique	Asymmetric key crypto system
B. Conventional encryption	Cipher text symbols and plain text symbols are same
C. Mono alphabetic cipher	Symmetric key crypto system
D. public key crypto system	Relative frequencies of English alphabets

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

2. _____ forms a barrier through which the traffic going in each direction must pass. CO5 [K_2]

a) Trusted systems b) Fire wall
c) virus d) Key loggers

3. Consider the following statements. CO1 [K_2]

1. Eavesdropping is updation of hacked message.
2. Stream cipher involves encrypting bulk plain text at a time.
3. Brute force attack is trying all possible keys to find out plain text.
4. Public key crypto system provides authentication.

Which of these statements are correct?

a) 1,3 b) 1,4

c) 1,2 d) 2,3

4. If an attacker can forge a signature for at least one message, but he/she does not have control over the message, then the attack is characterized as: CO2 [K_2]

a) Universal forgery c) Selective forgery

c) Masquerading forgery d) Existential forgery

5. Assertion: Hash function has one way property. CO3 [K_2]

Reason: for any given value h, it is computationally infeasible to find x such that H(x)= h.

a) Both A and R are Individually true and R is the correct explanation of A b) Both A and R are Individually true but R is not the correct explanation of A

c) A is true but R is false d) A is false but R is true

6. Which of the following is the open source software for e-mail security? CO4 [K_2]

a) Kerberos b) X.509

c) MIME d) PGP

7. Consider the following statements. CO2 [K_2]

1. Encryption of message using public key of receiver.
2. Decryption of encrypted message using public key of sender.
3. Encryption of message using private key of sender.
4. Decryption of encrypted message using private key of receiver.

The correct sequence to achieve confidentiality and authentication in a public key crypto system is

a) 2-3-4-1 b) 1-3-2-4

c) 3-4-2-1 d) 4-1-3-2

8. In CA hierarchy which action has to be performed when a user's private key is compromised? CO4 [K_2]

a) Generation of a new private key b) Certificate revocation

c) User renaming d) Generation of a new private/public key pair

9. Assertion: Public key crypto system is used mostly for key distribution and authentication. CO3 [K_2]

Reason: Slow compared to private key schemes.

a) Both A and R are Individually true and R is the correct explanation of A

b) Both A and R are Individually true but R is not the correct explanation of A

c) A is true but R is false

d) A is false but R is true

10. In which service the dual signature is used to provide security? CO5 [K_2]

a) Email security

b) secure electronic transactions

c) IP security

d) viruses

PART B (10 x 2 = 20 Marks)

(Answer not more than 40 words)

11. What is avalanche effect? CO1 [K_2]

12. Decrypt the following text using rail fence technique. CO1 [K_3]

sdioduaslanyhiy

13. Find the shift row transformation used in AES for the following matrix. CO2 [K_3]

45	3E	82	21
A7	59	94	4D
3A	1B	28	73
3F	2C	54	62

14. Write the Fermat's and Euler's throrem. CO2 [K_2]

15. What is the role of timestamp and challenge/response approaches in authentication protocols? CO3 [K_2]

16. Specify the requirements for message authentication. CO3 [K_2]

17. Draw the header format for an ISAKMP messages. CO4 [K_2]

18. What do you mean by 'Birthday attack' ? CO4 [K_2]

19. What are the metrics that are followed for profile based intrusion detection? CO5 [K_2]

20. What is meant by polymorphic viruses? CO5 [K_2]

Answer any FIVE Questions:-

PART C (5 x 14 = 70 Marks)

(Answer not more than 300 words)

Q.No. 21 is Compulsory

21. (a) Explain the RSA algorithm in detail. Perform encryption and decryption using RSA Algorithm with p=17, q=31, e=7,M=2. (8) CO2 [K_3]

(b) Give the detailed explanation about DES encryption algorithm (6) CO1 [K_2]

22. (a) Consider a diffie hellman scheme with the common prime q=11 and primitive root α = 2 (8) CO2 [K_3]

(1) Show that 2 is a primitive root of 11.

(2) If user A has public key $Y_A = 9$, what is the A' s private key X_A?

(3) If user B has public key $Y_B = 3$, what is the shared secret key K, shared with A?

(b) Write algorithm for the Key Expansion used in AES. (6) CO1 [K_2]

23. Encrypt the message "meet me at" using hill cipher with the following key and decrypt the same using inverse key. CO1 [K_3]

KEY: $\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$

24. Explain the concepts of SHA -1 in detail with their compression function CO3 [K_2]

25. How the authentication is ensured using Kerberos, explain with detail dialogue exchanges between server and workstation? CO4 [K_2]

26. How does PGP provide confidentiality and authentication service for e-mail and storage applications? Draw the block diagram and explain its components. CO4 [K_2]

27. Explain about intruders, intrusion techniques and approaches for intrusion detection. CO5 [K_2]

****