Register Number:……..

KUMARAGURU
college of technology
character is life

B.E DEGREE EXAMINATIONS: MAY 2018

(Regulation 2015)

Sixth Semester

COMPUTER SCIENCE AND ENGINEERING

U15CST603 : Cryptography and Network Security

COURSE OUTCOMES

CO1: Explain security issues and cipher techniques in computer systems and networks.
CO2: Explain the protocols for public key cryptography and make use of it to solve problems.
CO3: Outline the authentication functions.
CO4: Summarize the authentication and security protocols for real time applications.
CO5: Explain system level security issues.
CO6: Explain about various cyber crimes

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

Answer all the Questions:-

PART A (10 x 1 = 10 Marks)

1. Match List 1 – Security Services with List 2 – Security Mechanisms CO1 [K_2]

List I	List II
A. Confidentiality	i. Hashing
B. Integrity	ii. Redundancy
C. Authentication	iii. Encryption
D. Availability	iv. Kerberos

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

2. Tapping into as a third party and listening to a conversation between two individuals' is classified as ---------- CO6 [K_2]

a) Active attack b) Complex Attack
c) Passive Attack d) Simple Attack

3. Which of the following properties about one time pad are required to satisfy the unconditional (perfect) security requirements CO1 [K_1]

i) the key should be as long as the message
ii) the (same) key (sequence) should be used only once
iii) the key should be random

a) i and ii
b) ii and iii
c) i only
d) i, ii and iii

4. For achieving authentication, using RSA we should encrypt using _____ CO2 [K_2]

a) private key of the sender
b) public key of the sender
c) private key of the receiver
d) public key of the receiver

5. Assertion (A): It is better to use Asymmetric Key Cryptography where the sender and receiver do not trust each other rather than using Symmetric Key cryptography CO2 [K_3]
Reason (R): In symmetric key cryptography both sender and receiver has access to the same information whereas in asymmetric key cryptography either parties do not have to share their private keys with each other.

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. Give the correct sequence for digital signature creation and verification using the following modules: CO3 [K_2]
(i) Message and Hash Generation
(ii) Encrypt using Senders Private Key and Send
(iii) Receive and Decrypt using Senders Public Key
(iv) Compare Message / Hash with decrypted value and validate

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

7. Arrange the following in the sequence in which it happens: ---------- CO5 [K_2]
i) There is an attack
ii) There is a threat
iii) There is a vulnerability

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

8. Encapsulation Security Protocol (ESP) is used in ---------- CO5 [K_1]

a) PGP
b) IP Security
c) SSL
d) IDS

9. Assertion (A): E-certificates created using photo copy of the hand-written signatures of the signing authority and made as a PDF file are acceptable as verifiable digitally signed electronic record acceptable in the court of law. CO4 [K_4]
Reason (R): The e-certificate also contains the exact replica of the signature as in the paper certificate, and hence they are accepted in the court of law as a verifiable certificate.

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) Both A and R are false

10. How to validate a forensic image? CO5 [K_2]

a) by encryption

b) verify hash

c) by decryption

d) parity check

PART B (10 x 2 = 20 Marks)

(Answer not more than 40 words)

11. State the Shannon's principles of Diffusion and Confusion. CO1 [K_2]
12. Explain any one transposition cipher. CO1 [K_2]
13. List any four uses of (pseudo) random numbers in cryptography. CO2 [K_3]
14. State any one problem in Number Theory and its corresponding public key cryptographic algorithm. CO2 [K_2]
15. What is the difference between Hashing and Message Authentication Code? CO3 [K_2]
16. What is the difference between Message Authentication Code algorithm and Digital Signature? CO3 [K_4]
17. What is inter-realm authentication in Kerberos? CO4 [K_2]
18. How will you configure a Virtual Private Network based on IP Security protocol, between two private LANs interconnected using public internet? CO4 [K_3]
19. Explain any two rules of evidence. CO5 [K_2]
20. Is it possible to recover a file deleted from a system? Give a rationale to your answer. CO6 [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 AES algorithm in detail. (8) CO1 [K_2]

b. Explain Diffie Hellman Key Exchange Algorithm. (6) CO2 [K_2]

22. a. CSYFVSOIXLIGSHI – Suppose you have been given a clue that this may be a Caesar Cipher; find out the corresponding Plain Text and the key. (7) CO1 [K_3]

b. Present the Key Generation, Encryption and Decryption steps of RSA algorithm with an example. (7) CO2 [K_2]

23.	a. Explain the requirements that a good Hashing Algorithm must satisfy.	(6)	CO3	[K_2]
	b. Suppose your degree certificate is issued as digitally signed certificate, explain how that can be compromised by doing birthday attack on the underlying (say 64 bit) hashing algorithm.	(8)	CO6	[K_3]
24.	a. Differentiate between Digital Signatures and Digital Certificates (X.509)	(6)	CO3	[K_3]
	b. Explain PGP operation using a generic transmission and reception diagram	(8)	CO4	[K_2]
25.	a. Differentiate between statistical anomaly-based intrusion detection and rule-based intrusion detection	(6)	CO5	[K_3]
	b. List the different types of firewalls and explain about any one type	(8)	CO5	[K_2]
26.	a. For encrypting large messages will you use AES or RSA? Justify your answer	(7)	CO1 &2	[K_3]
	b. For providing non-repudiation will you use HMAC or DSA (Digital Signature Algorithm)? Justify your answer	(7)	CO3	[K_3]
27.	Explain the computer evidence processing steps.		CO6	[K_2]

****