Register Number:……..

KUMARAGURU
college of technology
character is life

B.E DEGREE EXAMINATIONS: MAY 2017

(Regulation 2014)

Sixth Semester

COMPUTER SCIENECE AND ENGINEERING

U14CST602 : Cryptography and Network Security

COURSE OUTCOMES

CO1: Explain security issues and objectives in computer systems and networks.
CO2: Explain the workings of fundamental cryptographic, authentication, network security and system security algorithms.
CO3: Identify the appropriate cryptography scheme & security mechanism for different computing environment and information systems.
CO4: Develop security protocols and methods to solve societal security problems.
CO5: Analyze security of network protocols and systems

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

Answer all the Questions:-

PART A (10 x 1 = 10 Marks)

1. Matching type item with multiple choice code CO2 [K2]

List I	List II
A. DES	i. Discrete Logarithms
B. AES	ii. Integer Factorization
C. RSA	iii. Fiestal Structure
D.ECC	iv. Galois Field

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

2. Hiding a small secret inside a large host file like an image is called_____ CO1 [K2]

a) Cryptography b) Hasing
c) Stegnography d) Encryption

3. Which of the following can be obtained using traffic analysis? CO1 [K2]

1. Identity of communicating hosts
2. Frequency of communication
3. Length of the message
4. Location of the communicating parties

a) 1,3,4 b) 1,4

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

4. Which of the following does not provide authentication? CO2 [K2]

a) DES b) RSA

c) AES d) Diffie Hellman Algorithm

5. Assertion (A): RSA is slow and computationally heavy. CO2 [K2]

Reason (R): Key size has to be sufficiently large in order to meet the security requirements.

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 about HMAC is NOT TRUE CO3 [K2]

a) Any secure Hash function can be used as part of it

b) The security of the HMAC is dependent on the security of the underlying Hash function

c) HMAC does not make use of key

d) HMAC makes use of hash function and a key

7. Give the correct sequence for digital signature creation and verification using the following modules: CO3 [K2]

(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)

8. In PGP for E-mail compatibility it uses _____ format. CO4 [K2]

a) ZIP b) radix-64

c) CAST-128 d) IDEA

9. Assertion (A): Digital Signature Standard cannot be used for encryption or key exchange CO3 [K2]
Reason (R): It is designed to provide only digital signature function.

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. Which of the following service is not addressed by IEEE 802.11i CO5 [K2]

a) Authentication
b) Integrity
c) Access Control
d) Destination non-repudiation

PART B (10 x 2 = 20 Marks)

(Answer not more than 40 words)

11. Construct a playfair matrix with the key 'examination'. CO1 [K2]
12. Distinguish between passive and active attacks. CO1 [K2]
13. State Fermet's theorem. CO2 [K2]
14. Why can't SHA be used for message authentication? Explain CO3 [K3]
15. Why are brute force attacks on MAC's considered more difficult than brute force attacks on Hash functions? CO3 [K3]
16. What is meant by inter-realm authentication in Kerberos CO4 [K2]
17. What do you mean by VPNs? CO4 [K2]
18. What is a honey pot? CO4 [K2]
19. List any four security threats specific to wireless networks. CO5 [K2]
20. Short notes on "WEP". CO5 [K2]

Answer any FIVE Questions:-

PART C (5 x 14 = 70 Marks)

(Answer not more than 300 words)

Q.No. 21 is Compulsory

21. With the neat diagram explain the algorithm Advanced Encryption Standard in detail. CO1 [K2]

22. With an example explain the key generation, encryption and decryption steps of the following algorithms. CO2 [K2]

i. RSA (7)
ii. Elliptic curve cryptography (7)

23.	Explain in detail about different approaches for providing message authentication.	CO3	[K2]
24.	Explain the methods of distribution of public keys analyzing the benefit of one over the earlier method.	CO2	[K2]
25.	Explain in detail about IP security	CO4	[K2]
26.	Write a short notes about the following	CO4	[K2]
	i. Firewall Types (7)		
	ii. Firewall Configuration (7)		
27.	Explain in detail about WAP protocol stack and compare it with TCP/IP and OSI models.	CO5	[K2]

****