Register Number:……………..

KUMARAGURU
college of technology
character is life

B.E DEGREE EXAMINATIONS: APRIL 2018

(Regulation 2014)

Eighth Semester

ELECTRONICS AND COMMUNICATION ENGINEERING

U14ECTE46**:** Network Security and Cryptography

COURSE OUTCOMES

CO1: Classify the symmetric encryption techniques.

CO2: Illustrate various Public key cryptographic techniques.

CO3: Evaluate the authentication and hash algorithms.

CO4: Discuss authentication applications

CO5: Summarize the 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. Match List I with List II CO1 [K_2]

List I	**List II**
A. Trap door	i. Denial of service
B. White hats	ii. Traffic analysis
C. Passive attack	iii. Secret entry point
D. Active attack	iv. Security Analysts

	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. In which block cipher mode technique the input to the encryption algorithm is the XOR of the next 64 bits of plaintext and the preceding 64 bits of cipher text ? CO1 [K_2]

a) Electronic codebook b) Cipher Feedback

c) Counter d) Cipher Block Chaining

3. Elliptic key encryption and decryption system requires the following parameters: CO2 [K_2]

1.Point G

2.Elliptic group $E_q(a,b)$

3.Private key n_A

4.Public key P_A

a) 1,3 b) 1,4

c) 1,2 d) 2,3

4. Calculation of secret key by user A in Diffie Hellman key Exchange is CO2 [K_2]

a) $K = (Y_B)^{XB}$ mod q b) $K = (Y_B)^{XA}$ mod q

c) $K = (X_A)^{XB}$ mod q d) $K = (Y_A)^{XA}$ mod q

5. Sequence the steps of HMAC algorithm: CO3 [K_2]

1.Append M to S_i

2.XOR K^+ with opad to get S_0

3.XOR K^+ with ipad to get S_i

4.Apply H to stream generated after appending M to S_i

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

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

6. Insertion of message into the network from a fraudulent source is known as --------------------- CO3 [K_2]

a) Masquerade b) Source repudiation

c) Destination repudiation d) Disclosure

7. Match PGP services with Algorithm Used: CO4 [K_2]

List I	**List II**
A. Digital Signature	i. Radix 64 conversion
B. Message Encryption	ii. ZIP
C. Compression	iii. CAST
D. E mail Compatibility	iv. DSS/SHA

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

8. Assertion (A): SMTP cannot transmit text data that includes national language characters. CO4 [K_2]

Reason (R): SMTP is limited to 7 bit ASCII

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

9. ------------------ is a form of virus explicitly designed to hide itself from detection by antivirus software. CO5 [K_2]

a) Parasitic virus

b) Memory resident virus

c) Boot sector virus

d) Stealth virus

10. Match generations with Anti virus software: CO5 [K_2]

List I	**List II**
A. First Generation	i. Activity traps
B. Second Generation	ii. simple scanners
C. Third Generation	iii. Full featured protection
D. Fourth Generation	iv. heuristic scanners

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

PART B (10 x 2 = 20 Marks)
(Answer not more than 40 words)

11. Decipher the following text using Caeser cipher technique “ DOO WKH EHVW” for the key K=3. CO1 [K_3]

12. List the four different stages in a single round of AES algorithm . CO1 [K_2]

13. Determine Φ(37) and Φ(35) CO2 [K_3]

14. List several techniques proposed for distribution of public keys. CO2 [K_2]

15. Define weak collision resistance and Strong collision resistance. CO3 [K_2]

16. State the requirements of digital signature. CO3 [K_2]

17. Compare transport mode and tunnel mode in IP Security Architecture. CO4 [K_2]

18. List the participants of Secure Electronic Transaction System. CO4 [K_2]

19. Who is a clandestine user? CO5 [K_2]

20. What are the four phases a virus undergoes during its lifetime. 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. Illustrate in detail a single round of Data Encryption Standard algorithm along with the key generation procedure with a neat diagram. Extend the same to general depiction of the algorithm diagrammatically. CO1 [K$_2$]

22. (i) Using the keyword "PROBLEMS" encrypt the following plain text "SHE WENT TO THE STORE" using play fair cipher technique. (7) CO1 [K$_4$]

    (ii) Using the key [1 3 (7)
    2 1] , encrypt the following text " DR GREER ROCKS" using HILL cipher.

23. The public key of a given user is e = 31, n = 3599. Calculate the private key of this user using RSA algorithm with detailed steps. (Note : Use Extended Euclid's algorithm). CO2 [K$_4$]

24. Outline the processing steps of single 1024 bit block of messages using SHA – 512 and also elementary SHA -512 operation for a single round with necessary equations and diagrams. CO3 [K$_2$]

25. What is Kerberos? Give an overview of it with neat diagrams. Summarize Kerberos version 4 message exchanges. CO4 [K$_2$]

26. Name the various approaches to Intrusion detection and briefly explain the same. CO5 [K$_2$]

27. List the design goals for a Firewall. Explain any two types of firewall with neat diagrams. CO5 [K$_2$]

****