KUMARAGURU college of technology
character is life

Register Number:……..…

M.E DEGREE EXAMINATIONS: JUNE 2015

(Regulation 2014)

Second Semester

COMMUNICATION SYSTEMS

P14COTE22**:** Communication Network Security

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

Answer all the Questions:-

PART A (10 x 1 = 10 Marks)

1. By applying permutation (31254) and substitution by 5 characters away from current character (A → F , B →G etc..) the following string ABRACADABRA becomes [K_3]

   a) FGWCAAADRBF
   b) RABCAAADRBF
   c) WFGHFFFIWGF
   d) ABCAAADRBFR

2. Which of the following are the solutions to network security? [K_2]

   i) Encryption
   ii) Authentication
   iii) Authorization
   iv) Non-repudiation

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

3. Triple DES uses [K_2]

   a) 168 bit keys on 64-bit blocks of plain text
   b) Working on 64-bit blocks of plain text and 56 bit keys by applying DES algorithm for three rounds.
   c) Works with 144 bit blocks of plain text and applies DES algorithm once.
   d) Uses 128 bit blocks of plain text and 112 bit keys and apply DES algorithm thrice.

4. Matching type item with multiple choice code [K_4]

List I	List II
A. Output Feedback (OFB)	i. bit errors do not propagate beyond the block
B. Electronic Code Book (ECB)	ii. Single bit error on c_j may only affect the corresponding bit of x_j
C. Cipher-Block Chaining (CBC)	iii. Single bit error on cj may flip the corresponding bit on x_j, but changes x_{j+1} significantly.
D. Cipher Feedback (CFB)	iv. bit errors (in ciphertext) propagate to the next block

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

5. DES and public key algorithm are combined [K_4]

(i) to speed up encrypted message transmission

(ii)to ensure higher security by using different key for each transmission

(iii) as a combination is always better than individual system

(iv) as it is required in e-Commerce

a) i and ii
b) ii and iii
c) iii and iv
d) i and iv

6. In public key encryption system if A encrypts a message using his private key and sends it to B [K_2]

a) if B knows it is from A he can decrypt it using A's public key
b) Even if B knows who sent the message it cannot be decrypted
c) It cannot be decrypted at all as no one knows A's private key
d) A should send his public key with the message

7. A hashing function for digital signature [K_4]

(i)must give a hashed message which is shorter than the original message

(ii)must be hardware implementable

(iii) two different messages should not give the same hashed message

(iv) is not essential for implementing digital signature

a) i and ii
b) ii and iii
c) i and iii
d) iii and iv

8. **Assertion (A):** The responsibility of a certification authority for digital signature is to authenticate the public keys of subscribers [K_4]

Reason (R) : Certification of Digital signature by an independent authority is needed because the authority checks and assures customers that the public key indeed belongs to the business which claims its ownership

a) Both A and R are true
b) Both A and R are false
c) A is false but R is true
d) R is true but A is false

9. In packet-filtering router, the following information can be external from the packet header. [K_4]

i) Source IP address ii) Destination IP address

iii) TCP/UDP source port iv) ICMP message type

v) TCP/UDP destination port

a) i, ii, iii and iv only b) i, iii, iv and v only

c) ii, iii, iv and v only d) All i, ii, iii, iv and v

10. An attempt to make a computer resource unavailable to its intended users is called [K_2]

a) denial-of-service attack b) virus attack

c) worms attack d) botnet process

PART B (10 x 2 = 20 Marks)

11. Why the product of two relatively simple ciphers, such as substitution and transposition achieves a high degree of security? [K_2]
12. Distinguish between cryptography and steganography. [K_4]
13. If a bit error occurs in plain text block P1, how far does the error propagate in CBC mode of DES and 8-bit CFB mode of DES? [K_2]
14. Compare and contrast steam ciphers from block ciphers. [K_4]
15. Draw a simple public key encryption model that provides both authentication and confidentiality. [K_2]
16. Define the one way property to be possessed by any hash function. [K_1]
17. Why the leading two octets of message digest are stored in PGP message along with the encrypted message digest? [K_2]
18. List the services are provided by Web Security. [K_2]
19. List at least 4 strategies for effective password management. [K_2]
20. Name the typical phases of operation of a virus or a worm. [K_1]

PART C (6 x 5 = 30 Marks)

21. Explain how Linear and Differential cryptanalysis are helpful in shortening an exhaustive search for determining the key size in DES. [K_4]
22. Let DES(x, K) represent the encryption of plaintext x with key K using the DES cryptosystem. Suppose DES(x, K) and y' = DES(c(x), c(K)), where c(.) denotes the bitwise complement of its argument. Prove that y' = c(y). [K_4]
23. Explain that the Electronic Code Book (ECB) mode is not a secured mode of encryption and highlight the problems with this mode [K_2]
24. List the main features of SHA- 512 Cryptographic hash function. What kind of compression function is used in SHA- 512 [K_2]

25. Let E be the elliptic curve $y2 = x^3 + x + 28$ defined over Z_{71}. [K_3]

i. What is the number of points on the curve?

ii. Is E a cyclic group?

iii. What is the maximum order of an element in E?

26. Why does PGP maintain key rings with every users? Explain how the messages are generated and received by PGP. [K_2]

PART D (4 x 10 = 40 Marks)

27. In AES, the size of the block is same as the size of the round key; in DES, the size of the block is 64 bits, but the size of the round key is 48 bits. What are the advantages and disadvantages of AES over DES with respect to this difference? Which algorithm will you prefer for securing your data? Give your arguments. [K_4]

28. The RSA public key cryptosystem is defined as follows: Let p and q be two prime numbers, let n = pq and $\varphi = (p-1)(q-1)$. Select a random integer e with $1 < e < \varphi$ such that $\gcd(e, \varphi) = 1$. Compute d such that $1 < d < \varphi$ and $ed \equiv 1 \pmod{\varphi}$. The public key is (n, e) and the corresponding private key is (n, d). The encryption of a message m is defined as $c = m^e \bmod n$ and the decryption is defined as $m = c^d \bmod n$. Answer the following question regarding RSA: [K_4]

A. Prove that decryption works.

B. Suppose that Alice and Bob use RSA public keys with the same modulus n, but with different public exponents e1 and e2. Prove that Alice can decrypt the messages sent to Bob.

C. Prove that Eve can decrypt a message sent to Bob and Alice if $\gcd(e1, e2) = 1$.

You may use Extended Euclidean Algorithm.

29. Mention the services provided by IP sec. Explain the two different modes of implementing IP security with appropriate diagrams. Compare the pros and cons of each. [K_2]

30. What is a firewall? Mention the limitations of a firewall. Explain in detail about the various ways of implementations of firewalls with appropriate diagrams. [K_2]

****