Regd No. □□□□□□□□□□

VIGNAN'S
Foundation for Science, Technology & Research
UNIVERSITY
(Estd u/s 3 of UGC Act of 1956)

Regulation: R13 **Code No: CS427/2**

IV B. Tech II Semester Examinations – April 2017

CRYPTOGRAPHY AND NETWORK SECURITY

(CSE)

Time: **3** hours Max. Marks: **60**

SECTION – A

(Short Answer Questions)

Answer all ten questions **10×1M=10M**

1. In computer security, means that computer system assets can be modified only by authorized parities.
   a) Confidentiality b) Integrity c) Availability d) Authenticity

2. The type of threats on the security of a computer system or network are:
   i) Interruption ii) Interception iii) Modification iv) Creation v) Fabrication
   a) i, ii, iii and iv only b) ii, iii, iv and v only c) i, ii, iii and v only d) All i, ii, iii, iv and v

3. DES is a(n) ________ method adopted by the U.S. government.
   a) symmetric-key b) asymmetric-key c) either (a) or (b) d) neither (a) nor (b)

4. DES uses a key generator to generate sixteen _______ round keys.
   a) 32-bit b) 48-bit c) 54-bit d) 42-bit

5. RSA encryption system is
   a) symmetric key encryption algorithm c) asymmetric key encryption algorithm
   b) not an encryption algorithm d) none of the mentioned

6. A digital signature is required
   (i) to tie an electronic message to the sender's identity
   (ii)for non-repudiation of communication by a sender
   (iii) to prove that a message was sent by the sender in a court of law
   (iv) in all e-mail transactions
   a) i and ii b) i, ii, iii c) i, ii, iii, iv d) ii, iii, iv

7. Pretty good privacy (PGP) is used in
   a) browser security b) email security c) FTP security d) none of the mentioned

8. PGP encrypts data by using a block cipher called
   a) international data encryption algorithm c) private data encryption algorithm
   b) intrenet data encryption algorithm d) none of the mentioned

9. The Secure Electronic Transaction protocol is used for
   a) credit card payment c) cheque payment
   b) electronic cash payments d) payment of small amounts for internet services

10. The following protocols and system are commonly used to provide various degrees of security services in computer network.
    i) IP filtering ii) Reverse Address Translation
    iii) IP security Architecture (IPsec) iv) Firewalls v) Socks
    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

SECTION – B

Answer all five questions **5×2M= 10M**

11. Explain the process of password protection.

12. Define the following keys used in PGP.
    I. One time session conventional key II. Public key
    III. Private key IV. Pass phrase based conventional key

13. It is possible to use a hash function to construct a block cipher with a structure similar to DES. Because a hash function is one way and a block cipher must be reversible (to decrypt), how is it possible?

14. We have shown that the Hill cipher succumbs to a known plaintext attack if sufficient plaintext-ciphertext pairs are provided. It is even easier to solve the Hill cipher if a chosen plaintext attack can be mounted. Describe such an attack.

15. Suppose H(m) is a collision resistant hash function that maps a message of arbitrary bit length into an n-bit hash value. Is it true that, for all messages x, x' with x≠ x', we have H(x) ≠H(x')? Explain your answer.

SECTION – C

Answer all four questions **4×5M = 20M**

16. Consider two parties trying to carry out a transaction via information channel which not secure. Establish a secure network model for carrying out transaction in such cases.

(OR)

17. Design a model for communication between two conventional cryptosystems.

18. Which parameters and design choices determine the actual algorithm of a Feistel cipher? Explain.

(OR)

19. Compute the bits number 1, 16, 33, and 48 at the output of the first round of the DES decryption, assuming that the ciphertext block is composed of all ones and the external key is composed of all ones.

20. Show that DES decryption is, in fact, the inverse of DES encryption.

(OR)

21. For feistel cipher it is stated that for the ideal block cipher, which allows all possible reversible mappings, the size of the key is n x 2n bits. But, if there are 2n ! possible mappings, it should take

log2 2n ! bits to discriminate among the different mappings, and so the key length should be log2 2n !. However, log2 2n !

22. In an RSA system, the public key of a given user is e = 31, n = 3599. What is the private key of this user? Hint: First use trail and error to determine p and q; then use the extended Euclidean algorithm to find the multiplicative inverse of 31 modulo φ(n).

(OR)

23. Suppose we have a set of blocks encoded with the RSA algorithm and we don't have the private key. Assume n = pq, e is the public key. Suppose also someone tells us they know one of the plaintext blocks has a common factor with n. Does this help us in any way?

SECTION – D

Answer all two questions **2×10M= 20M**

24. What are the roles of the Oakley key determination protocol and ISAKMP in IPSec?

(OR)

25. The IPSec architecture document states that when two transport mode SA's are bundled to allow both AH and ESP protocols on the same end-to-end flow, only one ordering of security protocols seems appropriate: performing the ESP protocol before performing the AH protocol. Why is this approach recommended rather than authentication before encryption?

26. In SSL and TLS, why is there a separate Change Cipher Spec Protocol, rather than including a change_cipher_spec message in the Handshake Protocol?

(OR)

27. List four techniques used by firewalls to control access and enforce a security policy.