Printed pages: 2	**MCAE21**
(The paper code and roll No. to be filled in your answer book)	
Roll No.	

MCA
(SEM V)ODD SEMESTER THEORY EXAMINATION, 2016-17

NETWORK SECURITY AND CRYPTOGRAPHY

Time: *3 Hours* ***Maximum Marks:*** *100*

Note:

(i) *Attempt all questions. All questions carry equal marks.*
(ii) *Notations/ Symbols/ Abbreviations used have usual meaning.*
(iii) *Make suitable assumptions, wherever required.*

Q.1. *Attempt any **FOUR** parts of the following:* **5x4=20**

a) Explain the following terms clearly.
Block Cipher, Non-repudiation, Denial of Service, Message Integrity, Traffic Analysis

b) How can meet in the middle attack be launched on Double DES?

c) Suppose that the plaintext **FD** is encrypted to **KJ** and **WA** is encrypted to **OG** using a 2 X 2 Hill cipher. Determine the key used.

d) Show that decryption in the Fiestal cipher structure is encryption of the ciphertext with reverse key schedule.

e) Describe the CFB and OFB modes of block cipher and highlight the relative advantages and disadvantages.

f) Discuss the merits and demerits of link level encryption and end-to-end encryption?

Q.2. *Attempt any **FOUR** parts of the following:* **5x4=20**

a) In an RSA scheme, given that global primes are **p = 7** and **q = 11** and the public key is e **= 17**. Determine the private key **d**.

b) Define group. Show that intersection of two subgroups of a group is also a subgroup while union of the same may not be.

c) Use Extended Euclidean Algorithm to find multiplicative inverse of 1234 mod 4321.

d) Explain the principle used in the design of S-Box of AES.

e) State and Prove Fermat's Theorem. Using Fermat's theorem, obtain $3^{201} \bmod 11$.

f) Use Chinese Remainder Theorem (CRT) to determine the value of **x** in the following simultaneous congruence.

$$x \equiv 4 \bmod 5,\ x \equiv 3 \bmod 7,\ x \equiv 1 \bmod 9,$$

Q.3. *Attempt any **TWO** parts of the following:* **10x2=20**

a)

(i) What of you understand by existential forgery in case RSA signature? How can it be tackled?

(ii) What is difference between strong collision resistance and weak collision resistance?

(iii) What is Steganography? Explain.

b) Write signature generation process of Elgamal Digital Signature Algorithm. What happens if the same value of ***k*** (user's secret number) is used to sign multiple messages using this scheme?

c) What is message authentication code (MAC)? What are the requirements of a message authentication code? Determine the value of ***n*** for which the probability that at least two messages in a set of ***n*** number of messages produces the same 512-bit hash value is 0.25.

Q.4. *Attempt any **TWO** parts of the following*: **10x2=20**

a) Give general structure of Public Key Ring and Private Key Ring of a Pretty Good Privacy mailing application and explain various attributes used the ring? Why does PGP use compression before enveloping the message?

b) Write Diffie-Hellman key exchange protocol and explain how is it vulnerable to the man-in-the-middle attack? Can you suggest some modification in the protocol to counter this attack?

c) What are the requirements defined for Kerberos. Explain the roles of authentication Server and ticket granting server. Write sequence of message exchanges in Kerberos and explain how it avoids traveling of plaintext password and handles possibility of the replay attack.

Q.5. *Write short notes on any **TWO** parts of the following:* **10x2=20**

a) Secure Socket Layer
b) Intrusion Detection
c) Virtual Private Network