COLLEGE OF ENGINEERING PUNE

(An Autonomous Institute of Govt. of Maharashtra)

END SEM - EXAM

Information Security (IT-14001)

Program: **B.Tech. (Information Technology)**
Year: 2014-15
Duration: 3 hr. 2:00 PM - 5:00 PM
Instructions:

Semester VII
Max. Marks: 60.

24 NOV 2014

1. **All Questions are Compulsory.**
2. **Make appropriate assumptions wherever necessary.**
3. **Give examples and draw neat diagrams wherever necessary.**

Q.1. A. Fill in the blanks and **Re-write** the complete sentence with correct answer: (5)

1. The first step in MD5 algorithm is ___________.
   a. Padding
   b. add length
   c. divide into subblocks
   d. initial permutation

2. The problem with Diffie-Hellman Key Agreement Protocol is _________________
   a. too short keys
   b. lack of security
   c. failure to agree on the key
   d. person in the middle attack

3. If we want to ensure the principle of ___________, the contents of a message must not change while in transit.
   a. Confidentiality
   b. Authentication
   c. Integrity
   d. Non–repudiation

4. The SET protocol uses the main principle of _________.
   a. digital signature

b. credit card payments

c. dual signature

d. digital certificates

5. In DES-3, we can use ___ or ____ keys.

a. 1 or 2

b. 3 or more

c. 1 or more

d. 2 or 3

B. Explain the zero point (point at infinity) of an elliptic curve? **(5)**

i) Does the elliptic curve equation $y^2 = x^3 + 10x + 5$ define a group over F_{17}?

ii) In the elliptic curve group defined by $y^2 = x^3 + x + 7$ over F_{17},

What is 2P if P = (1, 3)?

Q.2. A. List various ways of distribution of public keys. Explain each by taking appropriate example. **(5)**

B. What protocols comprise SSL? Describe the services provided by each protocol? **(5)**

Q.3. A. Decrypt the cipher text "EIS" using Hill Cipher technique where the key is ANOTHERBZ **(6)**

B. Using Euclid's Extended Algorithm, find the multiplicative inverse of **(2)**

i) 32 modulo 17 and ii) 17 modulo 32

C. Find the value of $\varphi(425)$ **(2)**

Q.4. A. Give example for each and explain the following attacks: **(5)**

i) man-in-middle attack ii) meet-in-the-middle attack

iii) Buffer overflow attack iv) Denial of Service attack

v) Phishing attack

B. Describe the X.509 Standard for PKI. Explain its structure (various fields). List some of the filename extensions for X.509 certificates. **(5)**

Q.5. A. Perform AES mix column transformation for following and show your calculations (5)

$$\text{Rcon}= \begin{matrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{matrix} \quad \text{State column} = \begin{matrix} 04 \\ 66 \\ 81 \\ E5 \end{matrix}$$

B. Describe digital signature. Explain the Digital Signature Algorithm and parameters involved in it. (5)

Q.6. A. With a neat structure of the classical Fiestel Network, explain the parameters and its design features in brief. Compare AES with Triple DES. (5)

B. Describe the need for firewall. What are the different types of firewalls? Explain each briefly. (5)