Comp / IT.

MIS Number

COLLEGE OF ENGINEERING, PUNE

(An Autonomous Institute of Govt. of Maharashtra)

ESE –Nov/Dec 2012

(CT-403) Information Security

Class: - Final Year B.Tech (Computer Engg. & Information Technology)

Year: - 2012-13 **Semester: - VII**

Duration: - 3 Hrs **Max. Marks: - 50**

Instructions:

1. ***All the Questions are compulsory.***
2. ***Assume suitable data whenever necessary.***
3. ***Draw neat figures wherever required***
4. ***Figures to right indicate full marks***

Q.1 a. Define an active attack. Explain any two active attacks with example. [3]

b. For transposition cipher the key is "heaven". Generate the plaintext for the ciphertext "ABEEESWHTTRE". [3]

c. Explain any two security services. [2]

Q.2. Answer the following: [10]

1. Find the GCD of 2740 and 1760 using Euclidian algorithm
2. Find and list all primitive roots of 17.
3. Why is SHA more secure than MD5?
4. Define meet in the middle attack.
5. What is the use of Needham-Schroeder Protocol?
6. Find the values of ø(243).
7. List the various steps of Computer Forensics.
8. List the various types of intruders.
9. Using Fermat's theorem, find 3^{220} mod 13
10. What is the difference between SHTTP and https?

Q.3. a. What is block cipher? Explain various block cipher modes of operations. [4]

b. In a public-key cryptosystem using RSA, you intercept the ciphertext C=284 sent to user whose public key is (e=223, n=713). What is the plaintext M? [4]

OR

b. Solve the following [4]

1. Does the elliptic curve equation $y^2 = x^3 - 7x - 6$ over real numbers define a group?
2. In the elliptic curve group defined by $y^2 = x^3 - 17x + 16$ over real numbers, what is 2P if P = (4, 3.464)?
3. Is (4,7) a point on the elliptic curve $y^2 = x^3 - 5x + 5$ over real numbers?
4. In the elliptic curve group defined by $y^2 = x^3 - 17x + 16$ over real numbers, what is P + Q if P = (0,-4) and Q = (1,0)?

Q.4. a. Draw the architecture of Secure Electronic Transaction (SET). Describe the working of its components. [4]

b. Explain the role of Ticket Granting Server in Kerberos. [4]

Q.5. a. Explain the transport and tunnel mode operation in Encapsulating Security Payload for IP security. [4]

b. How does PGP provide confidentiality and authentication service for e-mail and file storage applications? Draw the block diagram and explain its components. [4]

OR

b. Write the Digital signature algorithm Key Generation, Signature Creation and Signature Verification [4]

Q.6. a. What is cyber crime? List any two crimes which come under cyber crime? What are the objectives of IT act 2000? [4]

b. What are the different authentication procedures for X.509 certificates? Explain in detail. [4]