



Name : .....

Roll No. : .....

Invigilator's Signature : .....

**CS/M.TECH(CSE)/SEM-2/CST-42/2012**

**2012**

**INFORMATION SECURITY II**

*Time Allotted : 3 Hours*

*Full Marks : 70*

*The figures in the margin indicate full marks.*

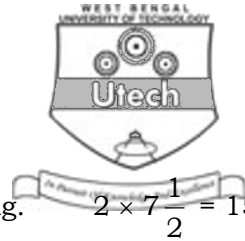
*Candidates are required to give their answers in their own words  
as far as practicable.*

**GROUP – A**

**( Short Answer Type Questions )**

Answer any *two* of the following :  $2 \times 5 = 10$

1. Describe Radix 64 in PGP.
2. Describe SHA-1 hash algorithm.
3. Describe selective encryption algorithm. In selective encryption, what is the main difference between the cases : if we apply compression first and then encrypt and encrypt first and then compress of some selective messages ?
4. How can you convert to a message to a point on an Elliptic curve ?



**GROUP – B**

Answer any *two* of the following.

$$2 \times 7 \frac{1}{2} = 15$$

5. What is Multi-proxy signature ? How is it differ from proxy signature ? Design a protocol for batch verification using a signature scheme, which can be applicable in VANET.

$$1 \frac{1}{2} + 2 + 4$$

6. Find addition of two same or different points on Elliptic curve. Let  $p = 23$  be a prime and consider the elliptic curve  $E : y^2 = x^3 + x + 4$  defined over  $\mathbb{F}_{23}$ . Find the points in  $E(\mathbb{F}_{23})$ .

$$2 \frac{1}{2} + 5$$

7. Consider an elliptic curve  $E : y^2 + xy = x^3 + \alpha^4 x^2 + 1$  over  $\mathbb{F}_{24}$ , where  $\alpha$  is primitive root of the irreducible polynomial  $x^4 + x + 1$ . Suppose a point  $P = (\alpha^6, \alpha^8)$  on the curve. Find what is  $2P$ . Describe an analogous of ElGamal encryption scheme in ECC.

$$5 + 2 \frac{1}{2}$$

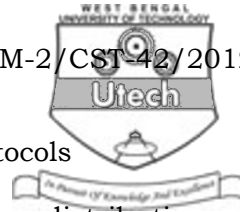
**GROUP – C**

**( Long Answer Type Questions )**

Answer any *three* of the following.

$$3 \times 15 = 45$$

8. a) Describe MD5 hash algorithm.  
b) Describe HMAC using MD5 for pseudorandom number generator.



- c) Describe SSL alert and handshake protocols
- d) Describe a mechanism for Quantum key distribution.

4 + 4 + 4 + 3

9. a) Describe AH format and ESP packet formats in IP Sec.
- b) Describe network based and host based Intrusion and Detection systems.
- c) Describe common modulus attack in RSA cryptosystem.

6 + 6 + 3

10. Define Bilinear pairings. Design a multi-signature scheme based on Bilinear pairings. Further describe a cryptosystem based on bilinear pairings.

2 + 7 + 6

11. a) What is SET ? Describe dual signature and its verification.
- b) Describe a method for ECDSA.
- c) Describe Kerberos V4 authentication protocol.

(2 + 3) + 5 + 5

---