6. (a) Draw a general diagram that depicts the processing of SHA-512. State the value of the padding field and length field in SHA-512 if the length of the message is 2942 bits.

(b) Define Mobile Security. Explain all security strategies of Mobile Devices.

(c) Define Pretty Good Privacy (PGP). Write the two significant differences between S/MIME and open PGP.

[This question paper contains 4 printed pages.]

Your Roll No.

Sr. No. of Question Paper : 1232 C

Unique Paper Code : 32357506

Name of the Paper : DSE-II Cryptography and Network Security

Name of the Course : **B.Sc. (H) Mathematics – (CBCS-Mode)**

Semester : V

Duration : 3 Hours Maximum Marks : 75

Instructions for Candidates

1. Write your Roll No. on the top immediately on receipt of this question paper.
2. **All** questions are compulsory.
3. Attempt any **five** parts from questions 1, each part carries **3** marks.
4. Attempt any **two** parts from questions **2** to **6**, each part carries **6** marks.

1. (a) Write a short note on Passive Attack in computer security.

(b) What is the difference between diffusion and confusion?

(c) What is an Avalanche effect? Which cipher DES or AES exhibit strong avalanche effect?

(d) Define discrete logarithm. Find discrete logarithm of every integer in (mod 5) with primitive root 3.

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

(f) Write the general equation of an elliptic curve. Define Elliptic curve $E_p(a,b)$ over Z_p.

2. (a) Define Symmetric encryption scheme also explain its five ingredients.

(b) Encrypt the message 'MONARCHY' using Hill Cipher with the key (7325).

(c) Explain Blum-Blum-Shub (BBS) pseudo-random bit generator and use it to produce a sequence of five random bits with p=13, q=7 and x=17.

3. (a) Find the solution of congruence $17x \equiv 9 (\text{mod } 276)$

(b) State the Fermat's theorem. Hence find $3^{201} \text{mod} 11$. Further prove the identity

$[(a \text{ mod } n)\ (b \text{ mod } n)](\text{mod } n) = (ab)(\text{mod } n)$.

(c) Explain the key generation in Data Encryption Standard (DES) with the help of a diagram.

4. (a) Find the multiplicative inverse of $x^5 + x^4 + x^2 + 1$ in $GF(2^8)$ with $m(x) = x^8 + x^4 + x^3 + x + 1$.

(b) Briefly describe AES Encryption Process with the help of a diagram.

(c) Perform encryption and decryption using the RSA algorithm for p = 5, q = 11, e = 3 and M = 6.

5. (a) Explain the Schnorr Digital Signature scheme.

(b) Consider the elliptic curve $E_7(2,1)$. Write the equation of the elliptic curve. Determine all of the points in $E_7(2, 1)$.

(c) Explain all S/MIME message-related services.

P.T.O.