Computer Science and Engineering Department, SVNIT, Surat
B.tech.-III, Semester-VI

Tutorial - 6

1. Calculate Cipher text C1 and C2 for plain text = 7 using Elgamal cryptosystem. Consider public key= (2,8,11), private key= 3 and r=4.
2. Explain the process involved in message digest generation and processing of single block in SHA-1.
3. Explain MAC based hash function with its design objectives and structure of the algorithm.
4. Given are two protocols in which the sender's party performs the following operation:

   Protocol A: y = ek1 (x||H(k2||x))

   where x is the message, H is a hash function such as SHA-1, e is a symmetric-key encryption algorithm, E is a public key encryption, "||" denotes simple concatenation, and k1, k2 are secret keys which are only known to the sender and the receiver.

   Protocol B: y = x, Ekpub (H(x)), where k is a shared secret key, and kpr is a private key of the sender (not shared with the receiver) and kpub is a public key of the receiver.

   a) Provide a step-by-step description (e.g., with an itemized list) of what the receiver does upon reception of y.

   b) State whether the following security services: • confidentiality • integrity • non-repudiation (preventing an entity from denying previous commitments or actions) is given for each of the two protocols given in the previous problem. You have to justify your answer.