Amrita Vishwa Vidyapeetham
B.Tech Computer Science and Engineering
Sixth Semester
15CSE341-Cryptography
Assignment 3

Part A

1. Prove the correctness of Elgamal signature verification

   (Hint. Prove that V1 = V2)

2. Alice and Bob are using Elgamal Digital Signature for communication. Alice chooses the value of q and α as 19 and 3 respectively. Illustrate the signature generation and verification process between Alice and Bob using a randomly selected private key. Here, Alice is the sender and Bob is the receiver

3. Suppose you are using CBC mode to compute hash function using block cipher E. Consider the encryption(here Encryption is equivalent to hash computation) of an n-block message $x = x_1||...||x_n$, by a block cipher E in CBC mode. We denote by $y = y_1||...||y_n$ the n-block ciphertext produced by the CBC encryption mode.

   (a) Show that one can extract information about the plaintext if we get a collision, i.e., if $y_i = y_j$with $i \neq j$.

   (b) What is the probability of getting a collision when the block size of E is 64 bits?

Part B

1. Consider a small chating program with two processes **A and B**, which includes following security features.

   (a) Symmetric key encryption for confidentiality(You can use any algorithm)

   (b) SHA-512 for integrity

   (c) HMAC for message authentication

   Write a program to implement this scenario(in any language with two participants). You are free to use library functions.