Assignment Number 6:

Implement a Public Key algorithm which works as following example:

Alice chooses pA = 107, αA = 2, dA = 67, and she computes βA = 267≡ 94 (mod 107). Her public key is (pA, αA, βA) = (2,67,94), and her private key is dA = 67.Bob wants to send the message "B" (66 in ASCII) to Alice. He chooses a random integer k = 45 and encrypts M = 66 as (r, t) = (αAk, βAkM) ≡ (245, 944566) ≡(28, 9) (mod 107). He sends the encrypted message (28, 9) to Alice. Alice receives the message (r, t) = (28, 9), and using her private key dA = 67 she decrypts to tr−dA= 9⋅28−67≡ 9⋅28106−67≡ 9⋅43 ≡66 (mod 107).

You may use any language to implement this example and verify your code with other values.

= 9to Alice

ElGamalCryptosystem- DecryptionSampleAlicereceives= 15and= 9fromBob.Herpublickey is(p; g; ga) = (17;6;7)Herprivatekey isa= 5Alicenow decryptsthemessageusingherprivatekey:Decryptionfactor(