## Homework 2

1. Use CRT to solve the following set of equations:

x = 5 mod 17

x = 9 mod 21

x = 7 mod 23

2. Using quadratic residues, solve the following congruences:

           a.   x2 ≡ 5 mod 11

3. S-AES

   a)  use the key 1010 0111 0011 1011 to encrypt the data block 0110 1111 0110 1011

   b)  use the same key 1010 0111 0011 1011 to decrypt the ciphertext  0000 0111 0011 1000

4.  Find the results of following, using Fermat's little theorem or Euler's theorem.

a)  1652381 mod 19

b) 78-1 mod 115

c) 45-1 mod 668

d) 19-1 mod 356

e) 3534994   mod 247

5. RSA

a) In a public key system using RSA, you intercept the ciphertext C=152 sent to Alice whose public key (11,221).  What is the plaintext M?

b) Suppose you intercept a message 39 with its signature 96 signed by Bob whose public key is (13, 209). You want to change the message 39 to 49. How do you create a valid signature for 49?

6. In ElGammal, given the prime p = 137, e1= 3

a) Choose a d and calculate e2

b) Choose a r (it's up to you to decide the value of r) and encrypt the message "happy"; use 00 to 25 for encoding.

c) Decrypt the ciphertext to obtain the plaintext

7. ElGamal signature scheme. Let p=881, e1 = 3, d=61. find  e2. Choose r (it's up to you to decide the value of r).

a)Find the values of s1 and s2  if M=400.

b) Verify the signature.

8. In the Diifie-Hellman protocol, g=7, p = 239, x = 18 and y=34.

a) What's the value of the symmetric key?

b) What's the value of R1 and R2?

9.DSS scheme. Let p = 743, q = 53, d = 56 and e0=5.  Find values of  e1 and e2. Choose  r = 17. Find the values of S1 and S2 if h(M) = 120. Verify the signature.