Homework 1

1. Use Euler's theorem to find the following results:

a). 17^{-1}mod 480

b). 11^{192002}mod 2800

2. Calculate the followings:

a) φ(228)

b) φ(445)

c) φ(302)

d) the order of the group <Z194*, x>

3. RSA. Alice wants to generate a pair of RSA public and private keys. She starts by selecting two primes p = 11 and q = 23. She selects e = 19. Suppose Bob's key pair is PUB=(17, 551), PRB=(89,551). (Note: PU means public key, PR means private key). Alice and Bob have already told each other's public key.

a) What are Alice's public key and private key?

b) Bob wants to send Alice a message M=25 which only Alice can read. What's the ciphertext C? After Alice receives C, how does she decrypt C to get M?

c) Bob sends the same M=25again to Alice. Bob wants to let Alice know that M is from him. How does he sign M? How does Alice verify the signature?

d) Alice wants to send Bob the message M = 25 to Bob. Now, she doesn't care about others reading M. She only wants to let Bob know that M is sent from her not from anyone else. How does she sign the M? How does Bob verify the signature?

4. Using the irreducible polynomial f(x) = x5+x2+1 to
a) generate the elements of the field GF(25)
b) based on the results of a), calculate
1) (x4 + x2 + 1)-1 MOD (x5 + x2 +1)
2) (x4 - x3 + 1) * (x3 + x2 + x + 1)
3) (x4 - x2 + 1) / (x3 + x2 + x + 1)

5. 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). Find the values of s1 and s2 if M=400. Verify the signature.

---

6. DSS scheme. Let p = 743, q = 53, d = 52 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.

---

7. Users A and B use the Diffie-Hellman key exchange technique with a common prime p=199 and a primitive root g = 6

a) If user A has private key x = 33, what is A's public key R1?

b) If user B has private key y = 49, what's B's public key R2?

c) How does A and B calculate the shared secret key?

d) If user C just joined the group and his private key is 18. What's the security key between A and C? What's the security key between B and C?

---

8. In a PGP community, the following trust relationship exits:

a) Alice fully trust John

b) Alice partially trust Cathy and Bob.

c) Alice doesn't trust Jason.

For each of the following successive events, give the content of Alice's public keying table. Note, it's up to you to choose the public key and the key ID of each person. You can ignore the timestamp field. The initial table is:

User ID	Key ID	Public Key	Producer trust	Certificate	Cert. trust	Key legit.
Alice	Alice1	111111	F			F

1) Alice called John to get John's public key and add it to the table.

2) Alice got Cathy's certificate issued by Bob and add her to the table

3) Alice received Bob's certificate issued by Cathy and add him to the table

4) Alice received Bob's certificate issued by John and add him to the table

5) Alice received Jason's certificate issued by Cathy.

6) Alice received Jason's certificate issued by Bob.

9. SET. Suppose PI = 71, OI =94. The hash function is h(x) = (x+11) mod 291. The customer's key pair is:
public key{17, 377}, private key{257, 377}. Concatenation works like this: 23||45 = 2345. Assume that both the merchant and the bank know the public key of the customer. The signature algorithm is RSA.

1) What's the dual signature created by the customer? Describe in detail how the customer create it.

2) What information does the merchant need to know to verify the dual signature and how to verify it?

3) What information does the bank need to know to verify the dual signature and how to verify it?

10.(AONDS) Alice has the following 4 12-bit secrets for sale:
S1=1091, S2=1472, S3=1461 S4=1168
Bob wants to buy S2 and Carol wants to buy S4.

The key pair for Bob is n=7387, e=5145, d=777. The key pair for Carol is n=2747,e=1421,d=2261. She tells Bob and Carol each their public key

Please describe step by step how Bob and Carol buy the secrets they want without letting Alice know which secrets they are buying.