Homework 2

1.(Shamir's secret sharing) Construct (4,5) threshold scheme to share a secret S = 15.

a) Create a secure polynomial.

b) Assign each participant a share.

c) Show how any 4 of the participant pool their shares to recover the secret S.

(Note: It's up to you to decide the values involved in the computation)

---

2. (Generalized secret sharing). Suppose there are 4 participants {P1, P2,P3,P4} and the access structure AS is { {P1, P2, P3}, {P2, P3,P4}, {P1,P4} }. Use Shamir's scheme to assign each participant share(s) so that only authorized group of participants can recover the secret.

(Note: you don't need to assign each participant specific values. Use s1, s2,... to denote the shares)

---

3. (Verifiable secret sharing). Construct a (4,4) verifiable threshold scheme to share a secret S=20.

a) How does the dealer construct a secure polynomial?

b) Assign each participant a share.

c) What information does the dealer publish?

d) How does each participant verify the validity of his/her share?

(Note: It's up to you to decide the values involved in the computation. Suppose p is large enough. You don't need a specific value for g)

---

4. (Proxy signature) In MUO's proxy signature scheme, p=241 and g=7. The original signer's private key x=14.
a) Generate a proxy key pair.
b) How does the proxy signer verify the validity of the proxy key pair?
c) The proxy signer needs to sign a message m=15 on behalf of the original signer. How does (S)he generate the proxy signature?
d) How does a verifier verify the proxy signature?

---

5. (Partially Blind signature) The signer's public key pair is (11,91) and he keeps (d,p,q)=(59, 7, 13) secure. A requester want the signer to sign m=19 with h(m)=23. The common information a is 25 with h(a) = 17.
a) How does the requester blind m and what information does he send to the signer? Suppose the two random numbers the requester selects are r = 3 and u=33.
b) After the signer receives the information sent by the requester, he selects a random number x=29 and send x the the requester. After the requester receives x, what does he do and what information does he send to the signer? Suppose the random number he selects is r' = 10.
c) How does the signer generate a blind signature?
d) After the requester gets the blind signature, how does he extract the signature?
e) How to verify the extracted signature?

---

6. In Tseng-Jan's group signature scheme, p=743, q=53, g=38. $h(x) = x^2 \bmod 100$. $a||b = a+b \bmod 100$. Suppose 2 users join a group, use specific values to show how the algorithm work(it's up to you to choose random values if required):

a) How the two users and the group manager (GM) set up the keys and other parameters

b) Suppose user 1 signs on a message M=20 on behalf of the group, what's the signature?

c) How to verify the group signature?

d) If there is a need to identify the signer, how to open the signature?

---

7. Secure multiparty communication. Assume the followings:

- RSA is used.
- Bob's public key is (19, 391)
- His private key is (315, 391)
- Alice's secret value i, is 5
- Bob's secret value j, is 8.
- Only the values from 1 to 10 are possible for i and j

Show how Alice and Bob knows which value is bigger without revealing their secret value to the other?

---

8. Prove that Chaum's undeniable signature scheme works, that is, the signature is valid if d= m^a * g^b mod p