Homework 2 solutions

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

a) Create a secure polynomial.

S = 15, t = 4, n = 5

Choose prime p = 17, p > max (S, n), define a_0 = S = 15

Choose t-1 = 3 independent coefficients (0 <= a_j <= p-1) : $a_1 = 3$, $a_2 = 5$, $a_3 = 7$

Create the secure polynomial over Z_{17}:

$f(x) = a_{t-1} x^{t-1} + \ldots + a_2 x^2 + a_1 x + a_0 \mod p$

$= 7x^3+5x^2 + 3x + 15 \mod 17$

b) Assign each participant a share.

x1 = 1, y1 = f(1) = 13 , assign share (1, 13) to participant 1;

x2 = 2, y2 = f(2) = 12 , assign share (2, 12) to participant 2;

x3 = 3, y3 = f(3) = 3 , assign share (3, 3) to participant 3;

x4 = 4, y4 = f(4) = 11, assign share (4, 11) to participant 4;

x5 = 5, y5 = f(5) = 10, assign share (5, 10) to participant 4;

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

c1= (-x2/(x1-x2))* (-x3/(x1-x3)) * (-x4/(x1-x4))

= (-2/(1-2)) * (-3/(1-3)) * (-4/(1-4))

= 2 * 3/2 * 4/3 = 4

c2= (-x1/(x2-x1))* (-x3/(x2-x3)) * (-x4/(x2-x4))

= (-1/(2-1)) * (-3/(2-3)) * (-4/(2-4))

= -1 * 3 * 2 = -6

c3= (-x1/(x3-x1))* (-x2/(x3-x2)) * (-x4/(x3-x4))

= (-1/(3-1)) * (-2/(3-2)) * (-4/(3-4))

= -1/2 * -2 * 4 = 4

c4= (-x1/(x4-x1))* (-x2/(x4-x2)) * (-x3/(x4-x3))

= (-1/(4-1)) * (-2/(4-2)) * (-3/(4-3))

= -1/3 * -1 * -3 = -1

S = c1y1 + c2y2 + c3y3 + c4y4 mod p

= 4*13 - 6*12 + 4*3 - 1*11 mod 17

= -19 mod 17 = -2 mod 17 = 15

---

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.

AS = { {P1, P2, P3}, {P2, P3,P4}, {P1,P4} }

AS = {{P1,P3},{P2,P3},{P1,P2},{P2,P4},{P3,P4}}

| AS | = 5

Use Shamir's (5,5) scheme to generate 5 shares S1,S2,S3,S4 and S5. Assign the shares in the following ways.

S1 --> P2, P4 S2 --> P1, P4

S3 --> P3, P4 S4 --> P1, P3

S5 --> P1, P2

So P1 has the shares {S2, S4, S5}, P2 has the shares {S1, S5}, P3 has the shares {S3, S4}

---

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?

S = 20 t = 4, n = 4

Choose prime p = 31, p > max (S, n), define $a_0 = S = 20$

Choose t-1 = 3 independent coefficients ($0 <= a_j <= p-1$) : $a_1 = 3$, $a_2 = 5$, $a_3 = 7$

Create the secure polynomial over ~~Z_{17}~~ $Z3_1$:

$f(x) = a_{t-1}\, x^{t-1} + \quad \ldots + a_2\, x^2 + a_1\, x + a_0 \mod p$

$= 7x^3+5x^2 + 3x + 20 \mod 31$

b) Assign each participant a share.

x1 = 1, y1 = f(1) = 4, assign share (1, 4) to participant 1;

x2 = 2, y2 = f(2) = 9 , assign share (2, 9) to participant 2;

x3 = 3, y3 = f(3) = 15 , assign share (3, 15) to participant 3;

x4 = 4, y4 = f(4) = 2, assign share (4, 2) to participant 4;

c) What information does the dealer publish?

$E(a0) = g^{a0} \mod p = g^{20} \mod p$

$E(a1) = g^{a1} \mod p = g^{3} \mod p$

$E(a2) = g^{a2} \mod p = g^{5} \mod p$

$E(a3) = g^{a3} \mod p = g^{7} \mod p$

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

Participant 1: (1,4)

$E(f(1)) = g^4$

$= E(ao) * E(a1) * E(a2) * E(a3) = g^{20} * g^3 * g^5 * g^7 = g^{35 \bmod 31} \bmod 31 = g^4 \bmod p$

Participant 2: (2,9)

$E(f(2)) = g^9$

$= E(ao) * E(a1)^2 * E(a2)^4 * E(a3)^8 = g^{20} * g^6 * g^{20} * g^{56} = g^{102 \bmod 31} \bmod 31 = g^9 \bmod p$

Participant 3: (3,15)

$E(f(3)) = g^{15}$

$= E(ao) * E(a1)^3 * E(a2)^9 * E(a3)^{27} = g^{20} * g^9 * g^{45} * g^{189} = g^{263 \bmod 31} \bmod 31 = g^{15} \bmod p$

Participant 4: (4,2)

$E(f(4)) = g^2$

$= E(ao) * E(a1)^4 * E(a2)^{16} * E(a3)^{64} = g^{20} * g^{12} * g^{80} * g^{448} = g^{560 \bmod 31} \bmod 31 = g2 \bmod p$

---

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.

Choose random number k = 50

$t = g^k \bmod p = 7^{50} \bmod 241 = 121$

$s = (x + kt) \bmod (p-1) = (14 + 50*121) \bmod 240 = 64$

The proxy key pair is (s,t) = (64, 121)

b) How does the proxy signer verify the validity of the proxy key pair?

The original signer's public key $y = g^x \bmod p = 7^{14} \bmod 241 = 188$

$g^s \bmod p = 7^{64} \bmod 241 = 94$

$yt^t \bmod p = 188*121^{121} \bmod 241 = 94$

$g^s \bmod p = yt^t \bmod p$, the proxy key pair (s,t) is verified.

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?

Select a random number r = 11

$S1 = g^r \bmod p = 7^{11} \bmod 241 = 68$

$S2 = (M-s*S1)\, r^{-1} \bmod p-1$

$= (15-64*68)*11^{-1} \bmod 240$

$= 223* 11^{-1} \bmod 240$

$= 223 * 11^{63} \bmod 240$

= 223 * 131 mod 240 = 173

($\varphi(240) = \varphi(2^4 * 3 * 5) = (2^4 - 2^3)*2*4 = 64$)

d) How does a verifier verify the proxy signature?

$g^m \bmod p = 7^{15} \bmod 241 = 111$

$(yt^t)^{S1} S1^{S2} \bmod p$

$= (188*121^{121})^{68} * 68^{173} \bmod 241$

$= 94^{68} * 74 \bmod 241 = 24 * 95 \bmod 241 = 111$

$g^m = (yt^t)^{S1} S1^{S2} \bmod p$, the proxy signature is verified.

---

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?

The requester chooses two random numbers: r= 3, u = 33

$\sigma = r^e h(m)(u^2+1) \bmod n$

$= 3^{11} * 23 * (33^2 +1) \bmod 91$

$= 61*23*89 \bmod 91$

$=15$

He send $(a, \sigma) = (25, 15)$ to the signer.

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?

The requester randomly choose a number r’ = 10

He calculates b = r * r’ = 2 * 10= 30

$\beta = b^e(u-x) \bmod n = 30^{11} * (33 – 29) \bmod 91 = 79$

He send $\beta = 79$ to the signer.

c) How does the signer generate a blind signature?

The signer computes: $\beta^{-1} \bmod n = 79^{-1} \bmod 91 = 79^{71} \bmod 91 = 53$

($\varphi(91) = \varphi(7 * 13) = 6 * 12 = 72$)

$t = h(a)^d (\sigma(x^2+1)\beta^{-2})^{2d} \bmod n$

$= 17^{59} (15 * (29^2 +1) 79^{-2})^{2*59} \bmod 91$

$= 75 * (15 * 842*53^2)^{118} \bmod 91 = 27$

The signer generates blind signature $(\beta^{-1}, t) = (53, 27)$, and send it to the requester.

d) After the requester gets the blind signature, how does he extract the signature?

The requester calculates:

$c = (ux+1) * \beta^{-1} * b^{e} \bmod n$

$= (33*29 +1) * 53 * 30^{11} \bmod 91 = (48*53 * 88) \bmod 91 = 12$

$S = t*r^{2}*r'^{4} \bmod n = 27 * 3^{2} * 10^{4} \bmod 91 = 27$

He extracts the signature (a, c, s) = (25, 12, 27)

e) How to verify the extracted signature?

To verify the signature, check $s^{e} = h(a)*h(m)^{2}*(c^{2}+1)^{2} \bmod n$?

$s^{e} = 27^{11} \bmod 91 = 27$

$h(a)*h(m)^{2}*(12^{2}+1)^{2} \bmod n$
$= 17*23^{2}*(12^{2}+1)^{2} \bmod 91$
$= 17*529*21025 \bmod 91$
$= 27$

The equation holds, so the signature is valid.

---

6. In Tseng-Jan's group signature scheme, p=743, q=53, g=38. $h(x) = x^{2} \bmod 100$. a||b = a+b mod 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):

Ack: The answer is from Yuan Yang.

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

U1: choose x1 = 3, y1= g^x1 mod p = 633;
U2: choose x2 = 5, y2 = g^x2 mod p = 162;
GM: x = 7 , y = g^x mod p = 626

U1 and U2 send their public key y1 and y2 to GM
GM choose k1 = 11 and k2 = 12 to U1 and U2

Calculate r1 and s1 for U1:

$r1 = g^{-k1} * y1^{k1} \bmod p = 65$
$s1 = (k1 - r1*x) \bmod q = 33$

Calculate r2 and s2 for U2:

$r2 = g^{-k2} * y2^{k2} \bmod p = 610$
$s2 = (k2 - r2*x) \bmod q = 35$

so U1 has (x1, y1, r1, s1) = (3,633, 65,33), U2 has (x2,y2,r2,s2) = (5, 162, 610,35);

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

U1 want to sign M=20, U1 random choose (a,b,d,t) = (3,5,12,9)

A = r1^a mod p = 65^3 mod 743 = 458;
C = (a*r1-d) mod q = (3*65-12) mod 53 = 24;
D = g^b mod P = 38^5 mod 743 = 162;
E=y^d mod p = 626^12 mod 743 = 663;
B = (a*s1-b*h(A||C||D||E)) mod q
= (3*33-5*49) mod 53
=13
$\alpha = g^{B} * y^{C} * E * D^{h(A|C|D||E)}$ mod p
= (38^13)*(626^24)*663*162^49 mod 743
= 388

R = α^{t} mod p
= 388^9 mod 743
= 675

S = t^{-1}(h(m||R)-R*x1) mod q = 6*(25-675*3) mod 53
= 31

The signature is (R,S,A,B,C,D,E) = (675, 31, 458, 13, 24, 162, 663)

c) How to verify the group signature?

$\alpha^{h(m||R)}$ mod p ? = $(\alpha * A)^{R} * R^{S}$ mod p

$\alpha^{h(m||R)}$ mod p = 388 ^ 25 mod 743 = 37

$(\alpha * A)^{R} * R^{S}$ mod p = ((388*458)^675) * 675^31 mod 743 = 37

So the group signature is valid

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

GM first calculates α = 388

GM identifies U1 because the following equation holds:
388 = $((g^{C} * E^{x^{-1}} \text{mod } q)$^$(r_{1}^{-1} * k_{1}$ mod q)) mod p
= $(38^{24} * 663^{38})^{31*11 \text{ mod } 53}$ mod 743
= (242*364)23 mod 743
= 388

---

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?

1) Alice chooses a large random number, x=193, and encrypts it in Bob's public key

$c=E_B(x) = 193^{19} \bmod 391 = 335$

E_B is the encryption algorithm with Bob's public key

2) Alice computes c-i = 335-5 = 330 and sends the results to Bob

3) Bob computes the following 10 numbers:

$y_u = D_B\,(c\text{-}i\text{+}u)$, for 1<=u<=10

u=1 $y_1 = D_B\,(330+1) = 331^{315} \bmod 391 = 257$

u=2 $y_2 = D_B\,(330+2) = 332^{315} \bmod 391 = 83$

u=3 $y_3 = D_B\,(330+3) = 333^{315} \bmod 391 = 122$

u=4 $y_4 = D_B\,(330+4) = 334^{315} \bmod 391 = 131$

u=5 $y_5 = D_B\,(330+5) = 335^{315} \bmod 391 = 193$

u=6 $y_6 = D_B\,(330+6) = 336^{315} \bmod 391 = 157$

u=7 $y_7 = D_B\,(330+7) = 337^{315} \bmod 391 = 333$

u=8 $y_8 = D_B\,(330+8) = 338^{315} \bmod 391 = 179$

u=9 $y_9 = D_B\,(330+9) = 339^{315} \bmod 391 = 135$

u=10 $y_{10} = D_B\,(330+10) = 340^{315} \bmod 391 = 374$

4) Bob chooses a large random prime p = ~~131~~ 137(<x)

5) Bob computes the following 10 numbers:

$z_u = (y_u \bmod p)$, for 1<=u<=10

u=1 $z_1 = y_1 \bmod p = 257 \bmod 137 = 120$

u=2 $z_2 = y_2 \bmod p = 83 \bmod 137 = 83$

u=3 $z_3 = y_3$mod p = 122 mod 137 = 122
u=4 $z_4 = y_4$mod p = 131 mod 137 = 131
u=5 $z_5 = y_5$mod p = 193 mod 137 = 56
u=6 $z_6 = y_6$mod p = 157 mod 137 = 20
u=7 $z_7 = y_7$mod p = 333 mod 137 = 59
u=8 $z_8 = y_8$mod p = 179 mod 137 = 42
u=9 $z_9 = y_9$mod p = 135 mod 137 = 135
u=10 $z_{10} = y_{10}$mod p = 374 mod 137 = 100

6) Bob verifies that, for all u≠ v

$| z_u – z_v | >= 2$ and that for all u
$0 < z_u < p-1$

Bob does all the verification and confirms that the sequence is fine

7) Bob sends Alice this sequence of numbers in this exact order

$z_1, z_2, \ldots, z_j, z_{j+1} +1, z_{j+2} +1, \ldots, z_{100} +1, p$
= 120, 83, 122, 131, 56, 20, 59,42, 135+1, 100+1, 137
= 120, 83, 122, 131, 56, 20, 59,42, 136, 101, 137

8) Alice checks whether the 5^{th} number is in the sequence is congruent to 193 mod 131.

56 = 193 mod 137
Alice knows that i <= j (5 < 8)

9) Alice tells Bob the result

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

d = c^t mod p

= c^(x^-1) mod p

= s^a(x^-1)*y^b(x^-1) mod p

= m^xa(x^-1) * g^xb(x^-1) mod p

= m^a * g^b mod p