Programming Test

Secure Multiparty Computation

- Yao's millionaire problem
  - Alice knows a secret – x, Bob knows a secret – y
  - Both together wants to know whether x>y, but none wish to reveal x or y
- Let, 1<= x,y <= 100, and Bob has public-private keys (PU_b and PR_b)

Alice

1. Compute C = E(PUb, M1), M1 -- a large random number
2. Compute C1 = C – x and sends C1 to Bob

Bob

3. Bob computes $M2_i$ = D(PRb,C1+i), for 1<= i <=100
4. Choose a large prime p (<M1); Bob can know the size of M1
5. Compute $Z_i = M2_i$ mod p, 1<=i<100
6. Verify if $|Z_i – Z_j|$ >= 2 for all (i,j) and 0 < Z_i < p-1, for all i, otherwise try another prime and repeat from step-4
7. Send to Alice the sequence: Z1, Z2,…, Z_y, Z_{y+1} +1, Z_{y+2} +1, …, Z100 + 1, p

Alice

8. Check if x-th number in the sequence is congruent to M1 mod p, if so, x <y, otherwise x>y
9. Alice tells the conclusion to Bob

Bob

10. Receive conclusion

Secure Multiparty Computation: example

Global: 1 <= x,y <=4

Alice (x = 4)

1. Compute C = E(PUb, M1) = 19, M1 = 39
2. Compute C1 = C – x = 15

Bob (y = 2): RSA with parameters PUb = 7 and PRb = 23, n =11

3. $M2_1$ = D(PRb,15+1) = 16; $M2_1$ = D(PRb,15+2) = 18; $M2_1$ = D(PRb,15+3) = 2; $M2_1$ = D(PRb,15+4) = 39
4. P=31;
5. Z_1 = 26 mod 31 = 26; similarly Z_2 = 18, Z_3 = 2, Z_4 = 8
6. Verify all the conditions
7. Send: (26, 18,2+1,8+1, 31

8. 4-th number (9) is not congruent to 39 (mod 31), hence x>y
9. Send result of x>y to Bob

10. Receive result of x>y