Keyul Shah
(1207713672)
Project 2 – Mental Poker
CSE 539: Applied Cryptography

Mental Poker

Tasks:-

1. **Socket communication**
   - Implemented UDP socket programming for communication between two players on same computer.

2. **Encryption implementation**
   - Encryption key will be enter by user such that the gcd of encryption key and prime number-1 is should be 1.
   - Encryption and decryption follow below equations.
     Encryption, $C = M^{E}_{A} \bmod n$
     Decryption, $M = C^{D}_{A} \bmod n$
     Here,
     C- Cipher text
     M- Plain text
     E_A - Encryption key
     D_A- Decryption key
     n – Prime no.

3. **Card selection and exchange using the encryption protocol**
   - User will enter the no. from where cards should be picks up for both players. 10 cards are pick up from entered no. First 5 cards are assign to Player A and other 5 cards are assign to Player B.
   - Cards are exchange at every required step by sendto() and rcvfrm() functions provided by socket program library.

4. **Verification of non-cheating once all cards are played**
   - Values for all cards are selected from 48 to 99. If cards numbers are assign from 1, it is very easy to predict some of cards because of encryption of small numbers. E.g. E(1) will give 1 so other player can easily guess the number and cards. Higher cards no. are difficult to decrypt without key.
   - At the end of game PlayerB (Bob) will send his decryption key to playerA (Alice) so playerA can verify all the cards of PlayerB. Because initially player A had chosen cards for both of them.

     This program follows the conditions,

     $E_A(E_B(M)) = E_B(E_A(M))$

     $D_A(D_B(M)) = D_B(D_A(M))$

Keyul Shah
(1207713672)
Project 2 – Mental Poker
CSE 539: Applied Cryptography

Functions:-

- void generateCard() – It will generate all cards for play.
- int gcd(int a , int b) – it will calculate gcd of encrypted key and primeno.-1 .
- int modPower(int msg,int key ,int primeNo) – it will encrypt/decrypt card with encrypted/decrypted key.
- int decKey(int a, int b)- it will generate decryption key for given encryption key.

Flow of program:-

On player B's output console

1. Enter Bob encryption key.
2. Program will generate decryption key for Bob and display it.
3. Cards are generated.
4. Cards are shuffled randomly.
5. Cards are encrypted with Bob encrypted key.
6. Cards are sent to Alice.

On player A's output console

7. Enter Alice encryption key.
8. Program will generate decryption key for Alice and display it.
9. Receive encrypted cards from Bob and display it.
10. Now enter no. for pickup cards from the deck.
11. Five cards are picked up for Alice.
12. Five cards are picked up for Bob.
13. Alice cards are encrypted with Alice encrypted key.
14. Bob cards are sent to Bob.
15. Alice cards are sent to Bob.

On player B's output console

16. Bob will receive both sets of cards.
17. Bob will decrypt his card with his decryption key.
18. Bob will decrypt Alice card with Bob's decryption key.
19. Bob's decrypted cards will display.
20. Bob will send Alice's cards to Alice.

On player A's output console

21. Alice will decrypt her cards with her decryption key.
22. Alice cards will be display.
23. Alice will receive Bob's Decryption key to verify Bob hasn't change his cards.
24. Alice decrypted bob's original card and display it.

Keyul Shah
(1207713672)
Project 2 – Mental Poker
CSE 539: Applied Cryptography

Instruction to run Program:-

1. Run project from folder Player B
2. Run project from folder Player A
3. Put two output console together.
4. Enter Bob Encrypted Key in Player B's output console
5. Enter Alice Encrypted Key in Player A's output console
6. Enter no. for pickup cards in Player A's output console

Notes:-

- Prime no. is same for both player and keep it fixed.
- Gcd of encrypted key and primeno.-1 should be 1. Otherwise it will give error.
- Player A is Alice.
- Player B is Bob.
- Both are used interchangeably.

Reference:-

- http://www.binarytides.com/programming-udp-sockets-c-linux/
- http://www.math.wustl.edu/~victor/mfmm/compaa/gcd.c
- https://myasucourses.asu.edu/bbcswebdav/pid-10121284-dt-content-rid-40702564_1/courses/2014Fall-T-CSE539-91371/mp.pdf