Project 2: Mental Poker

Submitted By: Akash Nishar (1207689739), Rahul Sharma (1206687439), Tejasvi Gangaiah (1207679274)

Mental Poker:

Mental Poker is a game played between two or more people. It is played without cards where the players have to select cards on the network and later publish their cards to decide who the winner is. This game uses SRA encryption/decryption algorithm for secure communication.

Approach:

Here we have user client/server approach where one of the player will be server and other will be client. So both will run the program. Here it is assumed that both client/server will be on same network and the firewall is turned off.

Socket Programming:

Socket Programming is an interface used by process or thread for communication over the network. We have used UDP protocol for this game because it is connectionless and no overhead of handshake between the server and client.

Encryption and Decryption:

Here encryption is done using SRA algorithm. In this algorithm, client will select a prime number of 15 to 16 bits and send it to server. Both server and client agree on the prime number and individually generate key pairs (encryption key, decryption key) which are co-prime to the (prime -1).

Keys: (encryptionKey x decryptionKey)mod(prime-1) = 1

Encryption: (message)^encryptionKey mod prime

Decryption: (encryptedMessage)^decryptionKey mod prime

Here the prime for both server and client should be same to follow the commutative property.

Cards:

Here in this game the cards value are defined from 47 to 99 where each card is given a face value and suit which is stored in another variable. So the card 47 is TWO OF HEARTS, 48 is THREE OF HEARTS... 99 is ACE OF SPADES.

Steps of Game:

1. Alice (server) will initialize the cards.
2. Bob (client) will connect to Alice and generate prime number.
3. Bob will send prime number to Alice.
4. Both generate individual key pairs for encryption and decryption.
5. Alice will shuffle the cards and encrypt it with his encryption key. Then it will send the encrypted cards to Bob.
6. Bob will select 5 cards for Alice and 5 cards for himself. He will encrypt his cards and send all 10 cards to Alice.
7. Alice will decrypt all 10 cards and send Bob's cards to Bob.
8. Bob will decrypt his cards.
9. Now both will bet on their cards.
10. One who is having high cards will win the game.

Game Rules:

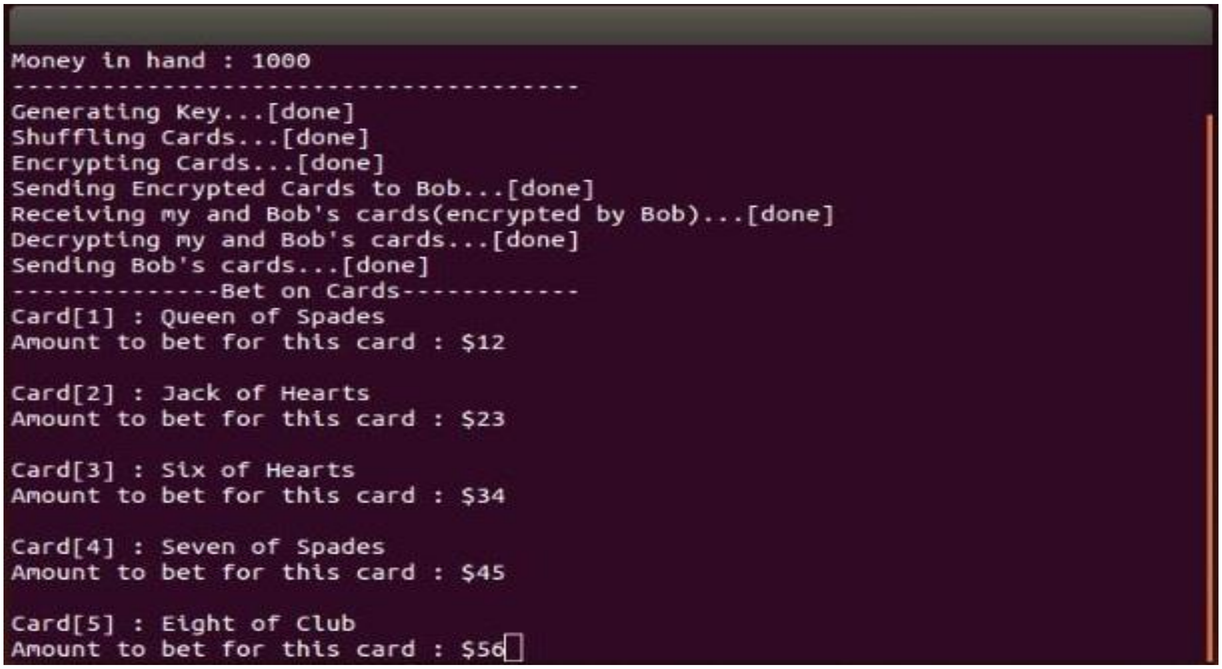
- Both players will start with $1000.
- Both players have to bid on each card.
- The card having higher face value will win the game. If cards have same face value the suits are taken into consideration. Here the priority is as follows: heart < club < diamond < spade.
- Player who wins more than 3 hands will win the game.
- The game will not stop until one of the player gets bankrupt.

Verification of cheating:

Here at the end of the game both players will exchange their decryption key. So the other player can verify the cards used by player are legitimate or not. Using the key it will decrypt the cards he/she previously have and match it with the cards player has used on the table. If there is any change in any card then the other player can know the cheating is done by other player.

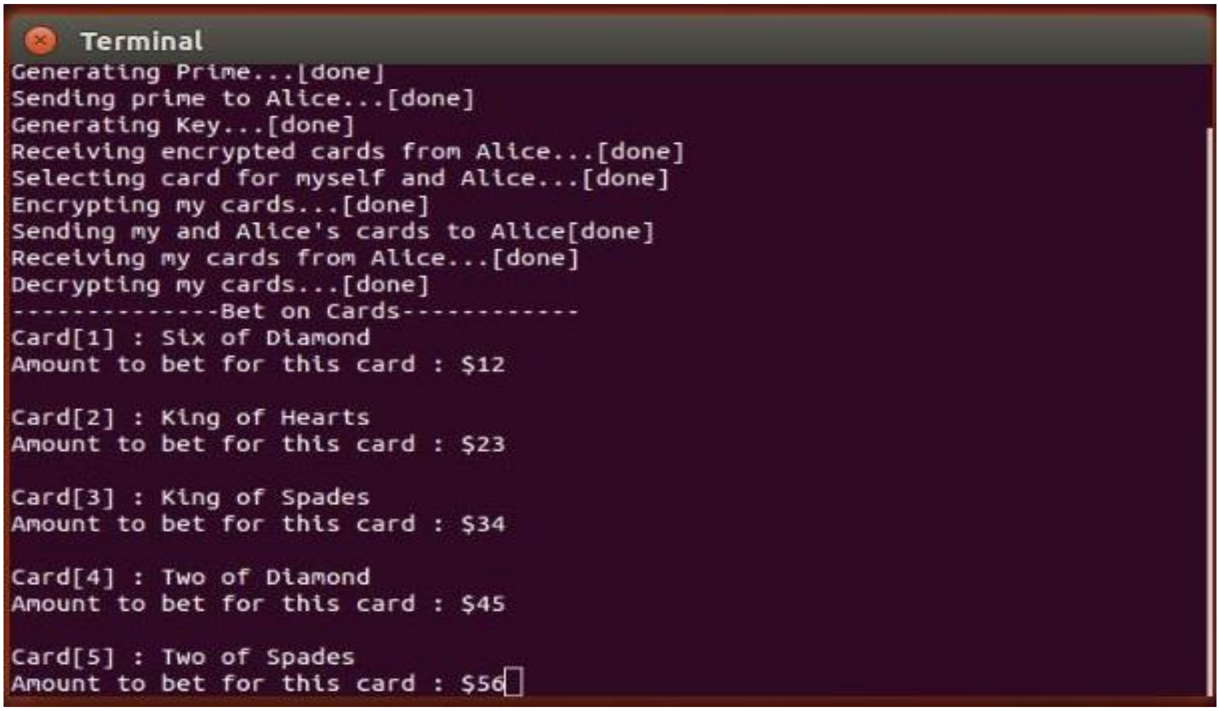
Screenshots:

Alice's Terminal



```
Money in hand : 1000
--------------------------------------
Generating Key...[done]
Shuffling Cards...[done]
Encrypting Cards...[done]
Sending Encrypted Cards to Bob...[done]
Receiving my and Bob's cards(encrypted by Bob)...[done]
Decrypting my and Bob's cards...[done]
Sending Bob's cards...[done]
--------------Bet on Cards------------
Card[1] : Queen of Spades
Amount to bet for this card : $12

Card[2] : Jack of Hearts
Amount to bet for this card : $23

Card[3] : Six of Hearts
Amount to bet for this card : $34

Card[4] : Seven of Spades
Amount to bet for this card : $45

Card[5] : Eight of Club
Amount to bet for this card : $56
```

Bob's Terminal



```
Generating Prime...[done]
Sending prime to Alice...[done]
Generating Key...[done]
Receiving encrypted cards from Alice...[done]
Selecting card for myself and Alice...[done]
Encrypting my cards...[done]
Sending my and Alice's cards to Alice[done]
Receiving my cards from Alice...[done]
Decrypting my cards...[done]
--------------Bet on Cards------------
Card[1] : Six of Diamond
Amount to bet for this card : $12

Card[2] : King of Hearts
Amount to bet for this card : $23

Card[3] : King of Spades
Amount to bet for this card : $34

Card[4] : Two of Diamond
Amount to bet for this card : $45

Card[5] : Two of Spades
Amount to bet for this card : $56
```

Assumptions:

- The communication channel is error free.
- The communication channel is reliable.
- No man in the middle attack possible.
- Only cheating can be done by players.

Result:

This program or game helped us to understand the concept of bit commitment protocol in cryptography. It also helped us to understand how two person without knowing each other can communicate securely and trustfully.