Program 13:

client.cpp -

```
#include <iostream>
#include <sys/socket.h>
#include <arpa/inet.h>
#include <string.h>
#include <stdio.h>
#include <stdlib.h>
#define SA struct sockaddr
using namespace std;

unsigned long powermod(unsigned long a, unsigned long b, unsigned long  q)
{
        unsigned long res=1;
        for(unsigned long i=0;i<b;i++)
                res=(res*a)%q;
        return res;
}

int main()
{


   int port;
   char addr[100]={'\0'};
   cout<<"Address  : "; gets(addr);
   cout<<"Port     : "; cin>>port;

        srand(time(NULL));
        unsigned long q, alpha, Xa, Ya, Yb, k;
        cout<<"q     = "; cin>>q;
        cout<<"alpha = "; cin>>alpha;

        Xa = rand() % (q-1) +1;
        Ya = powermod(alpha, Xa, q);

        // ****Connection
        struct sockaddr_in server={AF_INET, htons(port), inet_addr(addr)};
   int sockfd = socket(AF_INET, SOCK_STREAM,0);
   connect(sockfd, (SA*)&server, sizeof(server));
   // ****Connection Established


        send(sockfd, &Ya, sizeof(Ya), 0);
        recv(sockfd, &Yb, sizeof(Yb), 0);

        cout<< "Xa = " << Xa <<endl;
        cout<< "Ya = " << Ya <<endl;
        cout<< "Yb = " << Yb <<endl;
        k = powermod(Yb,Xa,q);
```

```
        cout<<"Key k = "<<k<<endl;

        unsigned long cipher;
        recv(sockfd, &cipher, sizeof(cipher), 0);
        unsigned long decipher=cipher^k;
        cout<<"Received message  : "<<cipher<<endl;
        cout<<"Decrpyted message : "<<decipher<<endl;

    close(sockfd);
    return 0;
}
```

server.cpp -

```
#include <iostream>
#include <sys/socket.h>
#include <arpa/inet.h>
#include <stdio.h>
#include <stdlib.h>
#include <math.h>
#define SA struct sockaddr
using namespace std;

unsigned long powermod(unsigned long a, unsigned long b, unsigned long  q)
{
        unsigned long res=1;
        for(unsigned long i=0;i<b;i++)
                res=(res*a)%q;
        return res;
}

int main()
{

    int port;
    char addr[100]={'\0'};
    cout<<"Address  : "; gets(addr);
    cout<<"Port     : "; cin>>port;

        srand(time(NULL));
        unsigned long q, alpha, Xb, Yb, Ya, k;
        cout<<"q     = "; cin>>q;
        cout<<"alpha = "; cin>>alpha;

        Xb = rand() % (q-1) + 1;
        Yb = powermod(alpha, Xb, q);

        // ****Connection
        struct sockaddr_in server={AF_INET, htons(port), inet_addr(addr)}, client;
    int sockfd = socket(AF_INET, SOCK_STREAM,0);
    bind(sockfd, (SA*)&server, sizeof(server));
    listen(sockfd,1);
```

```
    socklen_t len=sizeof(client);
    int connfd = accept(sockfd,(SA*)&client,&len);
    // ****Connection Established

        recv(connfd, &Ya, sizeof(Ya), 0);
        send(connfd, &Yb, sizeof(Yb), 0);

        cout<< "Xb = " << Xb <<endl;
        cout<< "Yb = " << Yb <<endl;
        cout<< "Ya = " << Ya <<endl;
        k = powermod(Ya,Xb,q);
        cout<<"Key k = "<<k<<endl;

        unsigned long msg;
        cout<<"Enter the msg to send : "; cin>>msg;
        unsigned long cipher=msg^k;
        send(connfd, &cipher, sizeof(cipher), 0);

        close(connfd);
    close(sockfd);
    return 0;
}
```

Output:

Server -

```
Address  : 127.0.0.1
Port     : 5000
q     = 71
alpha = 7
Xb = 21
Yb = 46
Ya = 20
Key k = 1
Enter the msg to send : 55
```

Client -

```
Address  : 127.0.0.1
Port     : 5000
q     = 71
alpha = 7
Xa = 40
Ya = 20
Yb = 46
Key k = 1
Received message  : 54
Decrpyted message : 55
```