PROGRAM:

Server:

```
#include <iostream>
#include <stdio.h>
#include <stdlib.h>
#include <ctype.h>
#include <arpa/inet.h>
#include <netinet/in.h>
#include <time.h>

using namespace std;

typedef long long int ll;

ll powermod(ll x,ll power,ll mod)
{
	int i=0;
	ll res=1;
	for(i=0;i<power;i++)
	{
		res=res*x;
		res=res%mod;
	}
	return res;

}

ll inverse(ll a,ll m)
{
	ll x=1,y=0;
	ll m0=m;
	if(m==1)
		return 0;
	while(a>1)
	{
		ll r = a%m;
		ll tempy=y;
		y=x-(a/m)*y;
		x=tempy;
		a=m;
		m=r;
	}
	if(x<0)
		x+=m0;
	return x;

}

int main()
{
```

```
srand(time(NULL));
int sockfd=socket(AF_INET,SOCK_STREAM,0),newfd;
ll pac[10];
struct sockaddr_in serv,clien;
socklen_t clen=sizeof(clien);
int port;
char ip[100]={'\0'};

printf("Enter the port no\n");
scanf("%d",&port);
printf("Enter the ip address\n");
scanf("%s",ip);

serv.sin_family=AF_INET;
serv.sin_port=htons(port);
serv.sin_addr.s_addr=inet_addr(ip);
bind(sockfd,(struct sockaddr*)&serv,sizeof(serv));
listen(sockfd,1);

newfd=accept(sockfd,(struct sockaddr*)&clien,&clen);
close(sockfd);
ll p,q,hash,h,g,y,x,k,s,r,M;

printf("Enter p and q\n");
scanf("%lld%lld",&p,&q);

printf("Enter the value of hash H(M) of the message\n");
scanf("%lld",&m);
hash=M^12;

h=rand()%(p-1);
if(h==1||h==0)
  h=2;

x=rand()%q;  //private key
if(x==0)
        x=1;

k=rand()%q;  //secret number
if(k==0)
        k=1;

ll num=(p-1)/q;
g=powermod(h,num,p);

y=powermod(g,x,p); //public key

r = powermod(g,k,p)%q;
s = (inverse(k,q)*(hash+x*r))%q;

pac[0]=hash;
pac[1]=y;
```

```
	pac[2]=r;
	pac[3]=s;
	pac[4]=g;

	printf("Packet sent with values: \nhash:%lld\npublickey(y):%lld\nr:%lld\ns:%lld\ng:
%lld\n",pac[0],pac[1],pac[2],pac[3],pac[4]);

	send(newfd,&pac,sizeof(pac),0);
	close(newfd);
	return 0;

}
```

Client:

```
#include <iostream>
#include <stdio.h>
#include <stdlib.h>
#include <ctype.h>
#include <arpa/inet.h>
#include <netinet/in.h>
#include <time.h>

using namespace std;

typedef long long int ll;

ll powermod(ll x,ll power,ll mod)
{
	int i=0;ll res=1;
	for(i=0;i<power;i++)
	{
		res=res*x;
		res=res%mod;
	}
	return res;

}

ll inverse(ll a,ll m)
{
	ll x=1,y=0;
	ll m0=m;
	if(m==1)
		return 0;
	while(a>1)
	{
		ll r=a%m;
		ll tempy=y;
		y=x+(a/m)*y;
		x=tempy;
		a=m;
		m=r;
```

```
	}
	if(x<0)
		x+=m0;
	return x;

}

int verify(ll p,ll q,ll hash,ll y,ll r,ll s,ll g)
{
	ll w = inverse(s,q)%q;
	ll u1= (hash*w)%q;
	ll u2= (r*w)%q;
	ll v = ((powermod(g,u1,p)*powermod(y,u2,p))%p)%q;
	printf("\nPost verification:\n v=%lld\n",v);
	if(v==r)
		return 1;
	else return 0;
}

int main()
{
	srand(time(NULL));
	int sockfd=socket(AF_INET,SOCK_STREAM,0);
	struct sockaddr_in serv;
	int port;

	printf("Enter the port number\n");
	scanf("%d",&port);
	char ip[100]={'\0'};
	printf("Enter the ip address\n");
	scanf("%s",ip);

	serv.sin_family=AF_INET;
	serv.sin_port=htons(port);
	serv.sin_addr.s_addr=inet_addr(ip);
	connect(sockfd,(struct sockaddr*)&serv,sizeof(serv));

	ll p,q;
	printf("Enter the value of p and q\n");
	scanf("%lld%lld",&p,&q);

	ll pac[10]={0};
	recv(sockfd,&pac,sizeof(pac),0);
	printf("Received\nhash:%lld\npublickey(y):%lld\nr:%lld\ns:%lld\ng:
%lld\n",pac[0],pac[1],pac[2],pac[3],pac[4]);

	if(verify(p,q,pac[0],pac[1],pac[2],pac[3],pac[4]))
		printf("Signature matched\n");
	else
		printf("Signature not matched\n");

	close(sockfd);return 0;
```

}

OUTPUT:

Server:

```
Enter the port no
7500
Enter the ip address
127.0.0.1
Enter p and q
10
20
Enter the value of hash H(M) of the message
14
Packet sent with values:
hash:2
publickey(y):1
r:1
s:19
g:1
```

Client:

```
Enter the port number
7500
Enter the ip address
127.0.0.1
Enter the value of p and q
10
20
Received
hash:2
publickey(y):1
r:1
s:19
g:1

Post verification:
 v=1
Signature matched
```