Laborator 6

1) Să se scrie un program pentru generarea cheilor pentru RSA.

Soluție:

```
# include "utile.h"

void main()
{
	citeste_alfabet();
	long p,q,n,phi,e,d;
	cout<<"Programul va genereaza o cheie pentru criptare;";
	srand((int)time(NULL));
	p=da_prim(3,215,0);//Generam numere astfel incat produsul a doua asemenea
numere sa nu depaseasca domeniul pentru variabile te tip int
	q=da_prim(3,215,p);
	n=p*q;
	phi=(p-1)*(q-1);
	e=3+rand()%(phi-3);
	d=invers(e,phi);
	while(d<0){//pentru ca e sa fie inversabil
		e++;
		d=invers(e,phi);
	}
	cout<<"\nCheia publica--> Ke=("<<n<<","<<e<<")";
	cout<<"\nCheia secreta--> Kd=("<<n<<","<<d<<")"<<endl;
}
```

2) Să se scrie un program pentru criptare/decriptare utilizând criptosistemul RSA.

Soluție:

Pentru criptare

```
# include "utile.h"

void main(){
	citeste_alfabet();
	int j,l,n,e,i,m;
	cout<<"Dati cheia publica:"<<endl;
	cout<<" n=";cin>>n;
	cout<<" e=";cin>>e;
	for(i=0,m=1;m<n;i++) m*=N;

	cout<<"\nDati lungimea blocului de caractere la citire(<="<<i<<")";
	cin>>j;
	cout<<"\nDati lungimea blocului de caractere la scriere(>="<<i<<")";
	cin>>l;
```

```
	char *c;
	ofstream out("destinatie.txt");
	ifstream in("sursa.txt");
	c=new char[l>=j?l:j];

	i=m=0;
	while(in>>noskipws>>c[i]){
		m=m*N+da_cod(c[i]);
		if (i==j-1){
			m=a_la_b_mod_c(m,e,n);
			i=l-1;
			while (m>0){
				c[i]=da_caracter(m%N);
				m=m/N;
				i--;
			}
			while (i>=0)c[i--]=da_caracter(0);
			for (i=0;i<l; i++)out<<c[i];
			i=0;
		}
		else
			i++;
	}
	out.close();
	in.close();
}
```