RSA

RSA este un algoritm de criptare folosind mecanismele de private/public key.

Pasi generare a public / private key:

1. Se aleg p si q 2 numere prime foarte mari.
2. Se calculeaza N = p * q
3. Se calculeaza $\lambda = (p - 1) * (q - 1)$
4. Se alege un E astfel incat cmmdc (E, λ) = 1. Altfel spus E si λ sunt numere coprime. $E < \lambda$
5. Se alege cel mai mic numar D astfel incat $E * D = \lambda * X + 1$. Sau altfel spus d este inversul multiplicativ a lui E modulo λ : $d*e \equiv 1 \pmod{\lambda}$
6. Perechea E, N se numeste cheie publica
7. Perechea D, N (sau D, P, Q) – se numeste cheie privata.
8. Pentru a encoda un mesaj M si a se obtine astfel mesajul C criptat se procedeaza:

   $C=M^E \bmod N$
9. Pentru a se face decodarea unui mesaj C si a se obtine mesajul initial M se procedreaza:

   $M=C^D \bmod N$

E.g.

p = 11 , q = 13 =>

N = p*q = 143

λ = (p-1)*(q-1) = 120.

Alegem E = 7. Calculam cel mai mic D astfel incat D*E = $\lambda * X + 1$. $D = 103$

$103 * 7 = 120 * 6 + 1$

Sa presupunem ca mesajul pe care vrem sa il criptam este M = 9 =>

$C=9^7 \bmod 143=48$

Ca sa decriptam:

$M=48^{103} \bmod 143=48$

Sugestii de implementare:

1. Codare

   Pe UI vor fii urmatoarele elemenete:

   - Button Load file – se va putea selecta orice tip de fisier pe care vreau sa il criptez
   - Posibilitatea de a introduce N si E. N si E vor fii numere care se vor putea stoca pe 32 de bits (fara semn).
   - Se va genera afisa un VECTOR de KEYS - de 8 Bytes (1 byte – 0..255) .
   - Button Crypt file – va face criptarea fisierului dat ca input. Extensia fisierului criptat va fii .myCrypt. Fisierul criptat va avea urmatoarea structura
     - Pe primii 4 octeti se va scrie in fisier E
     - Pe urmatorii 4 octeti se va scrie N
     - Fiecare element din KEYS va fii encoded aplicandui-se RSA. Rezultatul va fii scrii pe 32 de BITS in fisierul codat
     - Se va lua din fisierul original byte cu byte si se va face XOR cu KEYS [i++%8]. Astfel primul byte din fisier va fii facut XOR cu KEYS[0]. Rezultatul va fii scris in fisier. Apoi urmatorul byte din fiser va fii facut XOR cu KEYS[1]. Rezultatul va fii scris in fisier. s.a.m.d

2. Decodare

   Pe UI vor fii urmatoarele elemenete:

   1. Button Load file – se va putea selecta doar fisiere cu extensia *.myCrypt
   2. Posibilitatea de a introduce D (numar care va putea fii stocat pe 32 de BITS – fara semn).
   3. Button Decrypt file – va face decriptarea fisierului dat ca input. Extensia fisierului decriptat va fii .myDeCrypt. Algoritmul va face urmatorii pasi
      1. Pe primii 4 octeti din fisier citeste si afiseaza E
      2. Pe urmatorii 4 octeti din fisier citeste si afiseaza N
      3. Se vor citi cate 4 octeti. Fiecare element de catre 4 octeti va fii decodat aplicandu-se RSA. Se va obtine astfel vectorul initial de KEYS. Acesta trebuie afisat in mod read-only pe ecran.

4. Fiecare byte citit din fisierul codat se va face XOR cu KEYS[i] (decoded) si se va scrie in fisierul decodat. La sfarsit fisierul initial – dat la codare impreuna cu fisierul obtinut la decodare ar trebui sa fie identice.

Sample code how to compute RSA (simple way and a more fast way):

```
/*Raise B to the power X modulo N*/
RSA (B,X,N)
{
    R = 1; //!!! Probably R should be on 64 BITS unsigned
    for(k=1;k<=X;k++)
    {
        R*=B;
        R%=N;
    }

    return R;
}
```

```
/*Optimsed version Raise B to the power X modulo N*/
RSAOptimzed(B,X,N)
{
    R = 1; //!!! Probably R should be on 64 BITS unsigned
    while(X)
    {
        if (X % 2 == 1)
        {
            R*=B;
            R%=N;
        }
        B *=B;
        B %=N;
        X /= 2;
    }

    return R;
}
```