http://crypto.fmf.ktu.lt/xdownload/

- octave-7.3.0-w64-installer.exe
- octave.m.7z

CONSTRUCTION 11.32

Let **GenModulus** be a polynomial-time algorithm that, on input 1^n, outputs (N, p, q) where $N = pq$ and p and q are n-bit primes (except with probability negligible in n). Define a public-key encryption scheme as follows:

- **Gen:** on input 1^n run **GenModulus**(1^n) to obtain (N, p, q). The public key is $\langle N \rangle$, and the private key is $\langle N, \phi(N) \rangle$.
- **Enc:** on input a public key N and a message $m \in \mathbb{Z}_N$, choose a random $r \leftarrow \mathbb{Z}_N^*$ and output the ciphertext

$$c := [(1+N)^m \cdot r^N \bmod N^2].$$

- **Dec:** on input a private key $\langle N, \phi(N) \rangle$ and a ciphertext c, compute

$$m := \left[\frac{[c^{\phi(N)} \bmod N^2] - 1}{N} \cdot \phi(N)^{-1} \bmod N \right].$$

The Paillier encryption scheme.

$\phi(N) = \phi(p*q) =$
$= \phi(p) * \phi(q) =$
$= (p-1) * (q-1) =$
$\phi.$

- **Gen:** on input 1^n run **GenModulus**(1^n) to obtain (N, p, q). The public key is $\langle N \rangle$, and the private key is $\langle N, \phi(N) \rangle$.

$n = 14$

```
>> p=127
p = 127
>> isprime(p)
ans = 1
>> dec2bin(p)
ans = 1111111
>> q=113
q = 113
>> isprime(q)
ans = 1
>> dec2bin(q)
ans = 1110001
```

```
>> N=p*q
N = 14351
>> dec2bin(N)
ans = 11100000001111
>> N_2=int64(N*N)
N_2 = 205951201

>> fy=(p-1)*(q-1)
fy = 14112
```

```
>> p=genprime(7)

>> q=genprime(7)
```

- **Enc:** on input a public key N and a message $m \in \mathbb{Z}_N$, choose a random $r \leftarrow \mathbb{Z}_N^*$ and output the ciphertext

$$c := [(1+N)^m \cdot r^N \bmod N^2].$$

$e_1 \bmod N^2 \quad e_2 \bmod N^2$

$e_1 \cdot e_2 \bmod N^2$

```
>> m=11111
m = 11111  % m < N=14351

>> r=randi(N)
r = 9926
>> gcd(r,N)
ans = 1
```

$r \in \mathbb{I}_N^* = \{z, gcd(z,N)=1\}$

$gcd(r,N) = 1.$

```
>> e1=mod_exp((1+N),m,N_2)
e1 = 159453962
>> e2=mod_exp(r,N,N_2)
e2 = 67575538
>> c=mod(e1*e2,N_2)
c = 21508828
```

$c^{\phi} \bmod N^2 = d_1$

$\phi^{-1} \bmod N = d_3$

$$m := \left[\frac{[c^{\phi(N)} \bmod N^2] - 1}{N} \cdot \phi(N)^{-1} \bmod N \right].$$

$m = d_2 \cdot d_3 \bmod N$

$\frac{d_1 - 1}{N} \bmod N = d_2$

```
>> d1=mod_exp(c,fy,N_2)
d1 = 197426708
>> d1m1dN=mod((d1-1)/N,N)
d1m1dN = 13757
>> d2=mod((d1-1)/N,N)
d2 = 13757
>> d3=mulinv(fy,N)
d3 = 5224
>> mod(fy*d3,N)
ans = 1
>> mm=mod(d2*d3,N)
mm = 11111
```