We use toy example $|N^2| = 28 \Rightarrow |N| = 14 \Rightarrow |p| = |q| = 7$ bits

PuK = N --> **PrK = fy =** $\phi = (p-1)\cdot(q-1)$ $N = p \cdot q$; When $N \sim 2^{2048} \Rightarrow$ to find p, q is infeasible → RSA problem.

$m \in \mathcal{I}_N = \{0, 1, 2, \ldots, N-1\}$; $\mathcal{I}_N = \{0, 1, 2, \ldots, N-1\}$

$r \in \mathcal{I}_N^* = \{ z ; gcd(z, N) = 1 \}$; $\mathcal{I}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$

```
>> 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
>> dec2bin(N_2)
ans = 11000100011010010000011100001

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

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

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

(e_1, e_2)

$c = e_1 \cdot e_2 \bmod N^2$

```
>> m=11111
m = 11111
>> r=genprime(14)
r = 9049
>> gcd(r,N)
ans = 1

>> e1=mod_exp((1+N),m,N_2)
e1 = 159453962
>> e2=mod_exp(r,N,N_2)
e2 = 73833387
>> c=mod(e1*e2,N_2)
c = 120531541
```

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

(d_1; $d_2 \bmod N$; $d_3 \bmod N$)

$m = d_2 \cdot d_3 \bmod N$

```
>> d1=mod_exp(c,fy,N_2)
d1 = 197426708
>> d2=mod((d1-1)/N,N)
d2 = 13757
>> d3=mulinv(fy,N)
d3 = 5224
>> fy_m1=d3
fy_m1 = 5224
>> mod(fy*fy_m1,N)
ans = 1

>> mm=mod(d2*d3,N)
mm = 11111
```