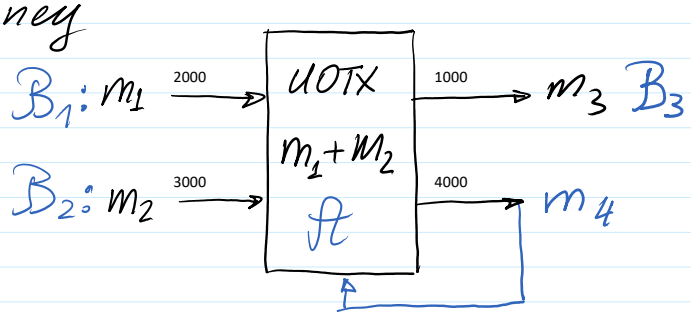
m_1, m_2 – certain sums of money

$$\left.\begin{aligned} m_i &= m_1 + m_2 \\ m_0 &= m_3 + m_4 \end{aligned}\right\} \; m_i = m_0$$



Transactions confidentiality

To hide sums $m_1 = 2000$; $m_2 = 3000$.

To provide confidential transactions numbers $n_1 = g^{m_1} \bmod p$ and $n_2 = g^{m_1} \bmod p$ are encrypted

$$n_1 \cdot n_2 \bmod p = (g^{m_1} \bmod p \cdot g^{m_2} \bmod p) \bmod p = g^{(m_1+m_2) \bmod p-1} \bmod p$$

$m_3 = 1000$; $m_4 = 4000$

$n_3 = g^{m_3} \bmod p$ and $n_4 = g^{m_4} \bmod p$.

$n_3 \cdot n_4 = g^{(m_3+m_4) \bmod (p-1)} \bmod p$ ⟸ Fermat theorem:

Operations in exponents can be reduced mod $(p-1)$ ⟸ If p – is prime: $z^{p-1} = 1 \bmod p \Rightarrow 0 \equiv p-1$

Paillier Encryption-Decryption

$N = p \cdot q$; $N^2 = p^2 \cdot q^2$; E.g. $p = 3$; $q = 5$; $N = 15$.

$f : \mathbb{Z}_N \times \mathbb{Z}_N^* \to \mathbb{Z}_{N^2}^*$; $\mathbb{Z}_N = \{0, 1, 2, \ldots, N-1\}$; $+ \bmod N$; $* \bmod N$

$\mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$; $\mathbb{Z}_N^* = \{z \mid \gcd(z, N) = 1\}$; $* \bmod N$

$\phi(15) = (3-1) \cdot (5-1) = 8$; $\mathbb{Z}_{N^2}^* = \{w \mid \gcd(w, N^2) = 1\}$; $\circledast \bmod N^2$

$\phi = (p-1) \cdot (q-1) = \phi(N)$: $\phi = (3-1) \cdot (5-1) = 2 \cdot 4 = 8$

$m \in \mathbb{Z}_N = \{0, 1, 2, \ldots, N-1\}$; $\mathbb{Z}_{15} = \{0, 1, 2, \ldots, N-1\}$

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

$m \in \mathbb{Z}_N = \{0, 1, 2, \ldots, N-1\}$; $\mathbb{Z}_{15} = \{0, 1, 2, \ldots, 14\}$

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

$|\mathbb{Z}_{15}^*| = 8$

$\gg \gcd(4, 15) = 1$

$\gg \gcd(9, 15) = 3 \neq 1.$

$\gg \gcd(7, 15) = 1$

To encrypt message m (probabilistically) the random number r must be generated: (m, r)

$Enc(k, r, m) = c = Enc(\phi, r, m)$

$k = \phi$

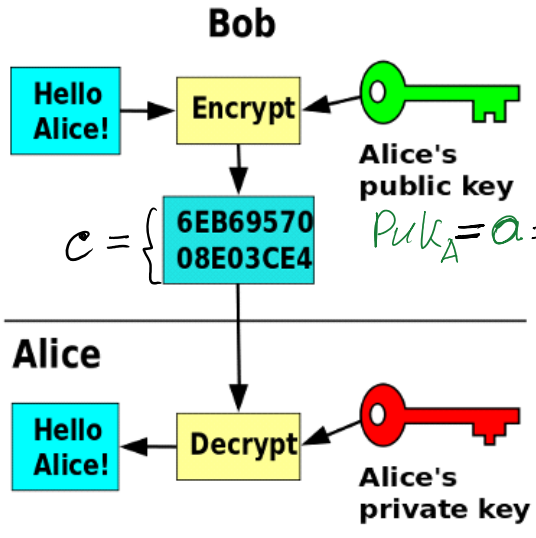
$(m, r) \in \mathbb{Z}_N \times \mathbb{Z}_N^*$;

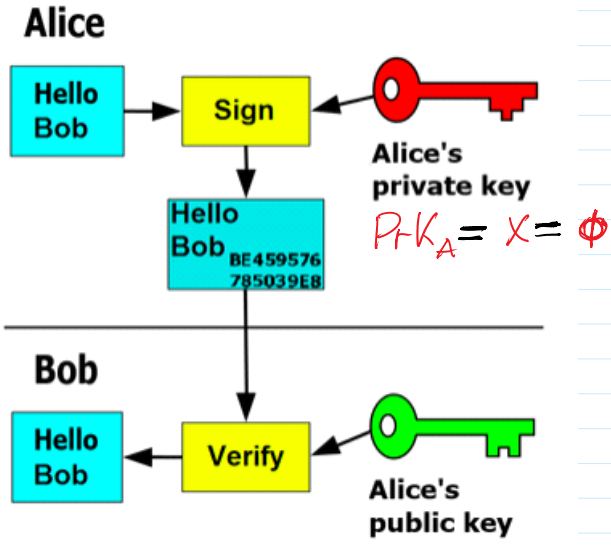
$c \in \mathbb{Z}_{N^2}^* = \{z ;\ \gcd(z, N^2) = 1\}$;

$Dec(N, c) = m \in \mathbb{Z}_N$.

$f : \mathbb{Z}_N \times \mathbb{Z}_N^* \longleftrightarrow \mathbb{Z}_{N^2}^*$; $f(m, r) = c$ $\quad Enc(PuK, m, r) = c$

$f^{-1} : \mathbb{Z}_{N^2}^* \longleftrightarrow \mathbb{Z}_N \times \mathbb{Z}_N^*$; $f^{-1}(c) = (m, r)$ $\quad Dec(PrK, c) = m$





$\phi(N) = \phi(p \cdot q) = \phi(p) \cdot \phi(q) = (p-1) \cdot (q-1) = \phi = PrK_A$

$\phi(N^2) = p \cdot (p-1) \cdot q \cdot (q-1) = p \cdot q \cdot (p-1) \cdot (q-1)$

$= |\mathbb{Z}_N| \cdot |\mathbb{Z}_N^*| = |\mathbb{Z}_N \times \mathbb{Z}_N^*| = |\mathbb{Z}_{N^2}^*|.$

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

Security:

When $PuK = N$ it is infeasible to find $\phi = (p-1) \cdot (q-1) \Rightarrow$

$\Rightarrow$ RSA problem is infeasible $\Leftrightarrow$ factorization problem.

>> factor(15) $\rightarrow$ ans 3, 5

Factorization problem is infeasible if N is sufficiently large.

$N \sim 2^{2048} \rightarrow |N| = 2048$ bits.

$f(m, r) = c \in \mathbb{Z}_{N^2}^*$ Encryption

$f^{-1}(c) = (m, r) \in \mathbb{Z}_N \times \mathbb{Z}_N^*$ Decryption

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 N, and the private key is $\langle N, \phi(N) \rangle = \langle N, \phi \rangle$.
- **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.

A : $PrK_A = x = \phi$. $PuK_A = a = N$. B : $PuK_A = a = N$; m – message to be

encrypted in dec. form: $m < N = pq$.

$Dec(\phi, c) = m$

$r \leftarrow randi(\mathbb{Z}_N^*)$

$\xleftarrow{c}$ $Enc(N, r, m) = c$

Probabilistic encryption:

Let $\mathcal{B}$ is encrypting message m (plaintext) 2 times.

1) $r_1 \leftarrow rand(\mathbb{Z}_N^*)$; $c_1 = (1+N)^m r_1^N \bmod N^2$

2) $r_2 \leftarrow rand(\mathbb{Z}_N^*)$; $c_2 = (1+N)^m r_2^N \bmod N^2$

$c_1 \neq c_2$ since $r_1 \neq r_2$.

Homomorphic property:

Paillier encryption is additively-multiplicative homomorphism.

Let m_1, m_2 – messages to be encrypted by $\mathcal{B}$.

r_1, r_2 – random numbers for encryption.

$Enc(N, r_1, m_1) = c_1$

$Enc(N, r_2, m_2) = c_2$

$Enc(N, r_1 \cdot r_2 \bmod N, m_1 + m_2 \bmod N) = c = c_1 \cdot c_2 \bmod N^2$

$c_1 = (1+N)^{m_1} \cdot r_1^N \bmod N^2$

$c_2 = (1+N)^{m_2} \cdot r_2^N \bmod N^2$

$$c_1 \cdot c_2 \bmod N^2 = (1+N)^{m_1} \cdot r_1^N \cdot (1+N)^{m_2} \cdot r_2^N \bmod N^2 =$$
$$= (1+N)^{m_1+m_2} \cdot (r_1 \cdot r_2)^N \bmod N^2 =$$
$$= Enc(N, \underbrace{r_1 \cdot r_2}_{r}, m_1 + m_2) = c$$

$Dec(\phi, c) = m_1 + m_2$

Shortcoming: Paillier encryption requires computations with large numbers taken mod N^2: $|N^2| = 4096$ bits.

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

eVoting: $Can1 := m_1$; $Can2 := m_2$; $Can3 := m_3$

Voters : $PuK = N$.

Election Commetee – EC

$PuK = N$; $PrK = \Phi$.

$V_1 : v_1 \in \{m_1, m_2, m_3\}$

$Enc(N, r_1, v_1) = c_1$ ——c_1——→

$V_2 : v_2 \in \{m_1, m_2, m_3\}$

$Enc(N, r_2, v_2) = c_2$ ——c_2——→

$V_N : v_N \in \{m_1, m_2, m_3\}$

$Enc(N, r_N, v_N) = c_N$ ——c_N——→ EC :

$c_1 \cdot c_2 \cdot \ldots \cdot c_N = c \bmod N^2$

$c = Enc(N, r, v)$

$r = r_1 \cdot r_2 \cdot \ldots \cdot r_N \bmod N$

$v = (v_1 + v_2 + \ldots + v_N) \bmod N$

EC: $Dec(\Phi, c) = v = (v_1 + v_2 + \ldots + v_N) \bmod N$

since $v_1 + v_2 + \ldots + v_n < N$

$v = v_1 + v_2 + \ldots + v_N$

Till this place

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

```
>> N=p*q
N = 14351
>> N_2=int64(N*N)
N_2 = 205951201
>> 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 = $(1+N)^m$, e_2 = r^N)

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

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

d_1

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

d_1

$d_2 \bmod N$ $\quad$ $d_3 \bmod N$

$m = d_2 \cdot d_3 \bmod N$

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

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

PROPOSITION 11.27 *Let $N = pq$, where p, q are distinct odd primes of the same length. Then:*

1. $\gcd(N, \phi(N)) = 1$.
2. *For any integer $a \geq 0$, we have $(1+N)^a = (1+aN) \bmod N^2$.*
   As a consequence, the order of $(1+N)$ in $\mathbb{Z}^*_{N^2}$ is N. That is, $(1+N)^N = 1 \bmod N^2$ and $(1+N)^a \neq 1 \bmod N^2$ for any $1 \leq a < N$.
3. *$\mathbb{Z}_N \times \mathbb{Z}^*_N$ is isomorphic to $\mathbb{Z}^*_{N^2}$, with isomorphism $f : \mathbb{Z}_N \times \mathbb{Z}^*_N \to \mathbb{Z}^*_{N^2}$ given by*

$$f(a, b) = [(1+N)^a \cdot b^N \bmod N^2].$$

[4] Recall that $\mathbb{Z}_N$ is a group under *addition* modulo N, while $\mathbb{Z}^*_N$ is a group under *multiplication* modulo N.

To show that f is an isomorphism, we show that $f(a_1, b_1) \cdot f(a_2, b_2) = f(a_1 + a_2, b_1 \cdot b_2)$. (Note that multiplication on the left-hand side of the equality takes place modulo N^2, while addition/multiplication on the right-hand side takes place modulo N.) We have:

mod N^2

$$f(a_1,b_1)\cdot f(a_2,b_2) = \left((1+N)^{a_1}\cdot b_1^N\right)\cdot\left((1+N)^{a_2}\cdot b_2^N\right) \bmod N^2$$
$$= (1+N)^{a_1+a_2}\cdot(b_1b_2)^N \bmod N^2.$$

Since $(1+N)$ has order N modulo N^2 (by Claim 11.29), we can apply Proposition 7.49 and obtain

$$f(a_1,b_1)\cdot f(a_2,b_2) = (1+N)^{a_1+a_2}\cdot(b_1b_2)^N \bmod N^2$$
$$= (1+N)^{(a_1+a_2 \bmod N)}\cdot(b_1b_2)^N \bmod N^2. \quad (11.8)$$

We are not yet done, since b_1b_2 in Equation (11.8) represents multiplication modulo N^2 whereas we would like it to be modulo N. Let $b_1b_2 = r + \gamma N$,

where γ, r are integers with $1 \le r < N$ (r cannot be 0 since $b_1, b_2 \in \mathbb{Z}_N^*$ and so their product cannot be divisible by N). Note that $r = b_1b_2 \bmod N$. We also have

$$(b_1b_2)^N = (r+\gamma N)^N \bmod N^2$$
$$= \sum_{k=0}^{N}\binom{N}{k} r^{N-k}(\gamma N)^k \bmod N^2$$
$$= r^N + N\cdot r^{N-1}\cdot(\gamma N) = r^N = (b_1b_2 \bmod N)^N \bmod N^2,$$

using the binomial expansion theorem as in Claim 11.29. Plugging this in to Equation (11.8) we get the desired result:

$$f(a_1,b_1)\cdot f(a_2,b_2) = (1+N)^{(a_1+a_2 \bmod N)}\cdot(b_1b_2 \bmod N)^N \bmod N^2$$
$$= f(a_1+a_2, b_1b_2),$$

proving that f is an isomorphism from $\mathbb{Z}_N \times \mathbb{Z}_N^*$ to $\mathbb{Z}_{N^2}^*$. ■

Encryption: m – message to be encrypted; $m \in \mathcal{I}_N$

$r \leftarrow randi(\mathcal{I}_N^*)$: $gcd(r,N)=1 \rightarrow r \in \mathcal{I}_N^*$

$Enc(a,m,r) = f(m,r) = c \in \mathcal{I}_{N^2}^*$.

$f(m,r) = (1+N)^m \cdot r^N \bmod N^2 = c \Leftarrow PuK_A = a = N.$

~~Due to isomorphism f: $c^\phi = (m,r)^\phi = (m\cdot\phi, r^\phi)$~~

$Dec(PrK_A = \phi, c) = m \Leftarrow PrK_A = \phi(N) = \phi = fy = (p-1)\cdot(q-1).$

Decryption. We now describe how decryption can be performed efficiently given the factorization of N. For c constructed as above, we claim that m is recovered by the following steps:

- Set $\hat{c} := [c^{\phi(N)} \bmod N^2]$.
- Set $\hat{m} := (\hat{c}-1)/N$. (Note that this is carried out over the integers.)

$c^{\phi(N)} = c^\phi \bmod N^2$

$5/4 = 1,25$

- Set $\hat{m} := (\hat{c} - 1)/N$. (Note that this is carried out over the integers.)
- Set $m := [\hat{m} \cdot \phi(N)^{-1} \bmod N]$.

To see why this works, let $c \leftrightarrow (m, r)$ for an arbitrary $r \in \mathbb{Z}_N^*$. Then

$$\begin{aligned}\hat{c} &\stackrel{\text{def}}{=} [c^{\phi(N)} \bmod N^2] \\ &\leftrightarrow (m, r)^{\phi(N)} \\ &= \left([m \cdot \phi(N) \bmod N], [r^{\phi(N)} \bmod N]\right) \\ &= ([m \cdot \phi(N) \bmod N], 1).\end{aligned}$$

By Proposition 11.27(3), this means that $\hat{c} = (1+N)^{[m \cdot \phi(N) \bmod N]} \bmod N^2$. Using Proposition 11.27(2), we know that

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

Since $1 + [m \cdot \phi(N) \bmod N] \cdot N$ is always less that N^2 we can drop the $\bmod N^2$ at the end and view the above as an equality over the integers. Thus, $\hat{m} \stackrel{\text{def}}{=} (\hat{c} - 1)/N = [m \cdot \phi(N) \bmod N]$ and, finally,

$$m = [\hat{m} \cdot \phi(N)^{-1} \bmod N],$$

as required. (Note that $\phi(N)$ is invertible modulo N since $\gcd(N, \phi(N)) = 1$.)

We give a complete description of the Paillier encryption scheme, followed by an example of the above calculations.

$5/4 = 1{,}25$

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

Euler T.: If $\gcd(r, \phi) = 1$, Then $r^{\phi} \bmod N = 1$

Fermat T.: If p is prime $\Rightarrow \forall r : r^{p-1} = 1 \bmod N$

$\phi(p) = p - 1$

$\hat{c} = m \cdot \phi \bmod N \Rightarrow m = \hat{c} \cdot \phi^{-1} \bmod N$

To find $\phi^{-1} \bmod N$

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 N, and the private key is $(N, \phi(N))$: $\phi(N) = \phi = f_\phi$.
- **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 $(N, \phi(N))$ 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.

B: PuK$_A$

A: PrK

$1^n = 1 \cdot 1 \cdot 1 \cdot \ldots \cdot 1$

n - required number of bits

$m < N$; $|N| = 2048$b.

Additively-Multiplicative encryption: v_1, v_2 - votes to be encrypted.

PuK $= N$; PrK $= \phi$.

Voter 1: $r_1 \leftarrow randi(\mathbb{Z}_N^*)$

$Enc(N, v_1, r_1) = c_1$

Voter 1: $r_2 \leftarrow randi(\mathbb{Z}_N^*)$

$Enc(N, v_2, r_2) = c_2$

$\Rightarrow c_1 * c_2 \bmod N^2 = Enc(N, v_1 + v_2, r_1 \cdot r_2)$

$gcd(r, n) = 1$

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

$f_1 = (1+n)^m \bmod n^2$

$f_2 = r^n \bmod n^2$

$c = (1+n)^m \cdot r^n \bmod n^2$

$f_1 \cdot f_2$

A: $Enc_{PuK_B}(m) = c$

$m \in M = \mathbb{Z}_N = \{0, 1, 2, \ldots, N-1\}$; $c \in C = \mathbb{Z}_{N^2}^*$

B: $Dec_{PrK_B}(c) = m$

ϕ^{-1} mod N computation with Octave software

```
>> fyem1 = mulinv(fy, N)
```

$$Enc(m_1 + m_2) = Enc(m_1) \cdot Enc(m_2) \quad \text{mod } N^2$$
$$c = c_1 \cdot c_2$$

$$Enc(m_1 \cdot m_2) = Enc(m_1) \cdot Enc(m_2)$$
$$Enc(m_1 + m_2) = Enc(m_1) + Enc(m_2)$$

} Full homomorphic (isomorphic)

Encrypted Data Base

$m_1 \longrightarrow$ randomas c_1

$m_2 \longrightarrow$ randomas c_2

Server - Cloud

(c)

$m_1, m_2 < N$

$Dec(c) = m_1 \cdot m_2$