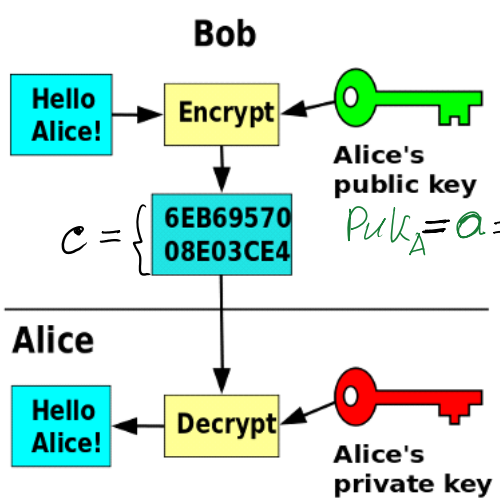

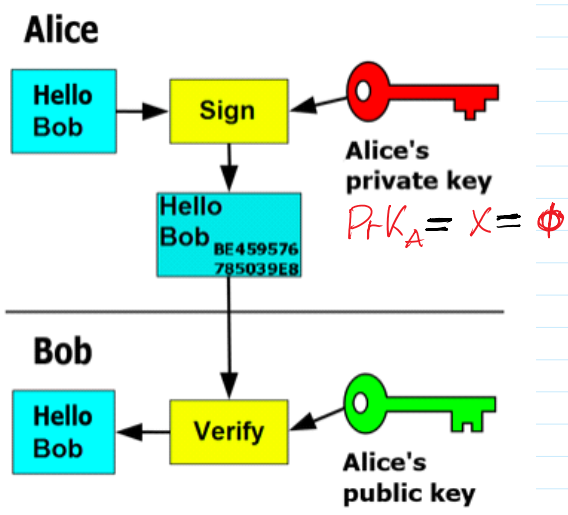

Paillier Encryption-Decryption

p, q – are primes of 1024 bits ⟹ $|N| = 2048$ bits

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

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

$\mathcal{Z}_p^* = \{1, 2, 3, \ldots, p-1\}$; $\mathcal{Z}_N^* = \{z \mid \gcd(z, N) = 1\}$; group: $* \bmod N$

$\mathcal{Z}_{N^2}^* = \{w \mid \gcd(w, N^2) = 1\}$; group: $\circledast \bmod N^2$

Example : $p = 15$

$\mathcal{Z}_{15} = \{0, 1, 2, \ldots, 14\}$; $\mathcal{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$;

$|\mathcal{Z}_{15}| = 15$ $|\mathcal{Z}_{15}^*| = 8$. Euler function $\phi(N) = \phi$

If $N = p \cdot q$ then $\phi(N) = (p-1) \cdot (q-1)$.

$\phi(15) = (3-1) \cdot (5-1) = 8$;

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

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

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

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

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

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

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

Euler function $\phi(\ )$:

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

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

$$= |\mathcal{I}_N| \cdot |\mathcal{I}_N^*| = |\mathcal{I}_N \times \mathcal{I}_N^*| = |\mathcal{I}_{N^2}^*|.$$

PuK = N --> PrK = fy = ϕ ; $N = p\cdot q$; When $N \sim 2^{2048} \Rightarrow$ to find p, q is infeasible → 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) → ans 3, 5

Factorization problem is infeasible if N is sufficiently large.

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

$\Psi_N(m, r) = c \in \mathcal{I}_{N^2}^*$ Encryption $\quad N^2 \sim 2^{4098}$; $|N| = 4096$ bits.

$\Psi_\phi^{-1}(c) = m \in \mathcal{I}_N$ 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.

$Enc_N(m, r) = c$

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

$Dec_\phi(c) = m$

$m = \dfrac{[c^\phi \bmod N^2]}{N} \cdot \phi^{-1} \bmod N$

We are using 28 bits arithmetic → $N^2 < 2^{28}$

>> p=127	>> N=p*q	>> m=11111	$c := [\underbrace{(1+N)^m}_{e_1} \cdot \underbrace{r^N}_{e_2} \bmod N^2].$
p = 127	N = 14351	m = 11111	
>> isprime(p)	>> N_2=int64(N*N)	% m<N	

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

N = 14351
>> N_2=int64(N*N)
N_2 = 205951201
>> fy=(p-1)*(q-1)
fy = 14112

m = 11111
% m<N

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

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

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

Task to verify the homomorphic property of Paillier encryption.

$m_1 = 11000 < N = 14112$

$\Psi_N(m_1, r_1) = Enc_N(m_1, r_1) = c_1$

$c_1 \in Z^*_{N^2}$; $* \bmod N^2$

$m_2 = 12000 < N = 14112$

$\Psi_N(m_2, r_2) = Enc_N(m_2, r_2) = c_2$

$c_2 \in Z^*_{N^2}$; $* \bmod N^2$

Compute $c_{12} = c_1 * c_2 \bmod N^2$

Decrypt ciphertext c_{12}: $Dec_\phi(c) = m_{12} = m_1 + m_2 = 13000$