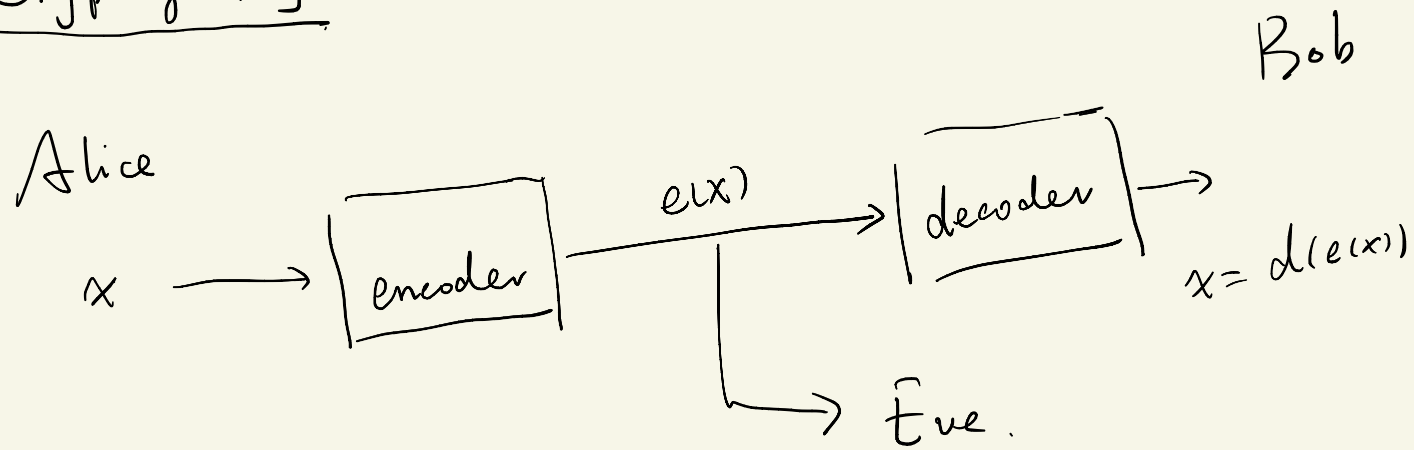
# Lec 2

## Algorithms with numbers

### Cryptography




private-key scheme

one-time pad $\quad e_r(x) = x \oplus r$

$\qquad\qquad\quad d_r(y) = y \oplus r$.

public key scheme.

RSA.

* Bob choose his public & secret key.

① pick two random n-bit prime p and q.

② $(N, e)$. $N = pq$, $e$ is relatively prime to $(p-1)(q-1)$

public key

③. secret key $d$: $ed = 1 \mod (p-1)(q-1)$.

* Alice sends $x$.

① $e(x) = x^e \mod N$.

② $d(y) = y^d \mod N$.

Example. $p = 5$, $q = 11$

$e = 3$.

$d = 3^{-1} \mod 40 = 27$.

* $y = x^3 \mod 55$

$x = y^{27} \mod 55$.

Prop.

① $x \to x^e$ is a bijection on $\{0, \dots, N-1\}$.

② $(x^e)^d = x \mod N$.

pf of ②. Since $ed = 1 \mod (p-1)(q-1)$

$\Rightarrow ed = k(p-1)(q-1) + 1$.

$(x^{ed} - x) \mod N$

$= x^{k(p-1)(q-1)+1} - x \mod (p \cdot q)$. $\cdots$ *

Fermat's little theorem $\Rightarrow$ (*) $= 0$.

$\forall a$: $a^{p-1} = 1 \mod p$.

## pf of FLT.

① $\forall\ 0 \le i, j \le p-1, \quad a \cdot i \neq a j \mod p.$

② $\{1, 2, \ldots, p-1\} = \{a \cdot 1, a \cdot 2, \ldots, a \cdot (p-1)\} \mod p$

③ $(p-1)! = a^{p-1} (p-1)! \pmod p$

④ $a^{p-1} = 1 \mod p.$

## Basic Arithmetic Operations

* Addition / Substraction. $O(n)$.

* Multiplication $O(n^2)$. $O(n \log n)$ using FFT. (next week).

* Modular arithmetic.

$x + y \mod N = (x \mod N) + (y \mod N) \mod N.$

$x \cdot y \mod N = \ldots$

fast exponentiation.

## division

$ax \equiv b \mod N$ has solution

$\Leftrightarrow \exists y \in \mathbb{Z}. \quad ax + Ny = b.$

$\Leftrightarrow \gcd(a,N) \mid b.$

pf. " $\Rightarrow$ " $\left.\begin{array}{l} \gcd(a,N) \mid ax \\ \gcd(a,N) \mid Ny \end{array}\right\} \Rightarrow \gcd(a,N) \mid b.$

" $\Leftarrow$ ". $g = \gcd(a,N).$

only need to prove $ax + Ny = g$ has an integral solution.

let $s \triangleq \min_{k>0} \{ ax + Ny = k$ has a integal sol $\}$.

$a = q_a s + r_a$ $\qquad$ $ax + Ny = s. \Rightarrow \gcd(a,N) \mid s.$

$N = q_N s + r_N$

$r_a = a - q_a s = a - q_a(ax + Ny)$

$= a(1 - q_a x) - q_a y \cdot N$

$\Rightarrow r_a = 0.$

* How to compute $\gcd(a, b)$.

Euclid $(a, b)$.

if $b = 0$ return $a$

return $\gcd(b, a \bmod b)$.

<u>Prop</u>. $a \geq b > 0$. $\gcd(a,b) = \gcd(a \bmod b, b)$.

Time $O(n^3)$.

<u>Extended Euclid.</u>

input $a, b$. find $ax + by = d$. $d = \gcd(a, b)$.

extended - Euclid $(a, b)$.

if $b = 0$. return $(1, 0, a)$.

$(x', y', d)$ = extended - Euclid $(b, a \bmod b)$

return $(y', x' - \lfloor a/b \rfloor \cdot y', d)$.

pf. Induction on $b$.

$b = 0$ ✓.

$$x' b + y'(a \bmod b) = \gcd(b, a \bmod b).$$

$$\Leftrightarrow \quad x' b + y'(a - \lfloor a/b \rfloor \cdot b) = d.$$

$$\Leftrightarrow \quad (x' - \lfloor a/b \rfloor y') b + y' a = d.$$

## Primality Testing.

Recall Fermat's little Thm.

$\forall$ prime $p$. $1 \le a \le p-1$. $\quad a^{p-1} \equiv 1 \mod p$.

**Prop.** If $N$ is not Carmichael & composite. $\geq$ the half of choices of $a$ satisfy $a^{N-1} \not\equiv 1 \mod N$.

pf. ① $\exists a$, $(a, N) = 1$ & $a^{N-1} \not\equiv 1 \mod N$.

② If $b^{N-1} \equiv 1 \mod N$, then

$$(a \cdot b)^{N-1} \equiv a^{N-1} \cdot b^{N-1} \not\equiv 1 \mod N.$$

③. $\forall\, i \not\equiv j \mod N$

$a \cdot i \not\equiv a \cdot j \mod N$.

Randomized algorithm.

Carmichael? Rabin-Miller.