Gems of TCS

Public Key Cryptography

Sasha Golovnev

April 15, 2021

SKC Secret key
Symmetric

$G(K) \oplus m$

Alice $\longleftrightarrow$ Bob

$\boxed{K}$ $\boxed{K}$

PKC Public key
Asymmetric

$\boxed{pk}$

Alice
$pk, \boxed{sk}$

Enc(pk, m) Bob ^{pk}

Enc(pk, m) Charlie ^{pk}

pk is sufficient for encrypting in order to decrypt, one needs sk

Eve, she can encrypt messages, but not decrypt.

SKC and PKC

SKC

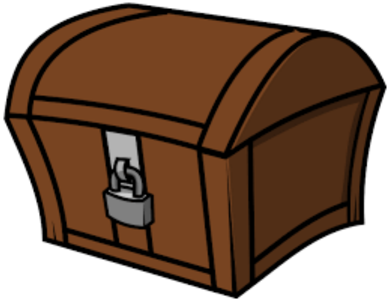
box with a lock,
Alice & Bob have key

SKC and PKC

PKC

box with padlock,

Alice has key (sk)

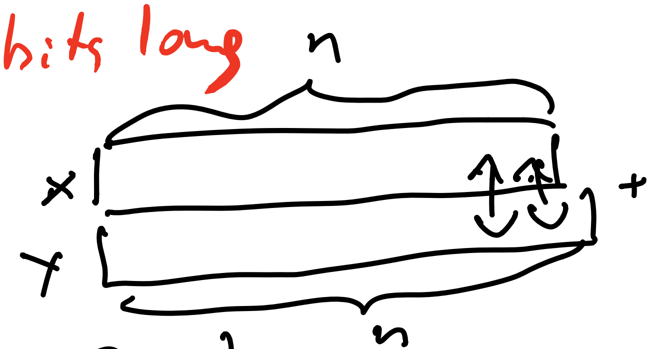


(Computational) Number Theory

$0 \le x, y < 2^n$

~ n bits long

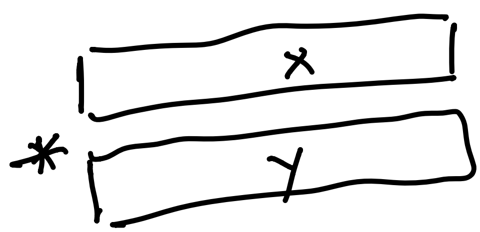
$x + y$



$O(n)$

$x - y$ $\quad O(n)$

$x \cdot y$?



standard alg: multiplies each digit of x with each dig y

$O(n^2)$

Karatsuba's alg.

$$12|345 * 67|890$$

$$(12 \cdot 1000 + 345) * (67 \cdot 1000 + 890)$$

$$= (\boxed{12 \cdot 67}) \cdot 10^6 + (\boxed{12 \cdot 890} + \boxed{345 \cdot 67}) \cdot 10^3$$

$$+ (\boxed{345 \cdot 890})$$

$T(n)$ - time complexity of multiplying two n-bit numbers

$$T(n) \leq 4T(n/2) + O(n) \leq$$

$$\leq O(n^2)$$

Karatsuba: (1960):

$a_1 = 12 \cdot 67$

$a_2 = 345 \cdot 890$

$a_3 = (12 + 345)(67 + 890)$

$= \underline{12 \cdot 67} + 12 \cdot 890 + 345 \cdot 67 + \underline{345 \cdot 890}$

$a_3 - a_1 - a_2 = 12 \cdot 890 + 345 \cdot 67$

$$T(n) \leq 3T(n/2) + O(n)$$

$$= n^{\log_2 3} \approx \underline{\boxed{n^{1.585}}} << n^2$$

Karatsuba is practical

In theory, we know multiply two numbers in time $O(n \log n)$

this constant is VERY large

$x + y$ $O(n)$

$x - y$ $O(n)$

$x \cdot y$ $n^{1.585}$ in practice

$n \log n$ in theory

GCD – greatest common divisor

Euclid's algorithm

$GCD(x, y)$ in time $O(n^2)$

$GCD(18, 24) = 6$

$GCD(7, 13) = 1$

integers (possibly neg)

Euclid's alg gives us $\boxed{a, b}$:

$$x \cdot a + y \cdot b = GCD(x, y)$$

$x = 18$ $y = 24$ $\Rightarrow$ $a = -1$, $b = 1$

$$xa + yb = 6 = GCD(x, y)$$

Modular Arithmetic

N – positive integer

p – prime

$\mathbb{Z}_N = \{0, 1, 2, \ldots, N-1\}$ with arithmetic is modulo N

$N = 12$

$5 + 11 = 4$ in $\mathbb{Z}_{12}$

$5 \cdot 7 = 11$ in $\mathbb{Z}_{12}$

$3 - 7 = 8$ in $\mathbb{Z}_{12}$

Modular inversion

Given x, find y s.t.

$$x \cdot y = 1 \text{ in } \mathbb{Z}_N$$

$$y = x^{-1} \text{ – inverse of } x$$

For example, N is odd integer
What is inverse of 2 in $\mathbb{Z}_N$?

$$\frac{N+1}{2} \in \mathbb{Z}_N$$

$$\frac{N+1}{2} \cdot 2 = N+1 = 1 \text{ in } \mathbb{Z}_N$$

If N is even, what's inverse of 2 in $\mathbb{Z}_N$? There's no inverse

$$\underline{2 \cdot y} = \underline{1} \text{ in } \underline{\mathbb{Z}_N}$$

Which els of $\mathbb{Z}_N$ have inverse?

Lemma $x \in \mathbb{Z}_N$ has inverse iff

$$GCD(x, N) = 1$$

Proof: If $GCD(x, N) = 1 \Rightarrow$ Euclid's alg gives a, b s.t.

$$x \cdot a + N \cdot b = 1$$

$$x \cdot a = 1 - \underline{N \cdot b} = 1 \quad \text{in } \mathbb{Z}_N$$

a is inverse of x in $\mathbb{Z}_n$.

If $GCD(x, N) > 1 \Rightarrow$

$$GCD(x \cdot a, N) > 1 \Rightarrow$$

$$x \cdot a > 1 \quad \text{in } \mathbb{Z}_N \qquad \square$$

Cor: If x has inverse in $\mathbb{Z}_N$, then we can find it in $O(n^2)$ by Euclid's alg.

$\mathbb{Z}_N = \{0, 1, 2, \ldots, N-1\}$ modulo N

$\mathbb{Z}_N^* =$ (set of invertible el's in $\mathbb{Z}_N$)

$= \{x \in \mathbb{Z}_N : \underline{GCD(x, N) = 1}\}$

$N = 12$

$\mathbb{Z}_N = \{\underline{0}, 1, 2, \ldots, 11\}$

$\mathbb{Z}_N^* = \{1, 5, 7, 11\}$

N = prime

$\mathbb{Z}_N = \{0, 1, 2, \ldots, N-1\}$

$\mathbb{Z}_N^* = \{1, 2, \ldots, N-1\} = \mathbb{Z}_N \setminus \{0\}$

Fermat's Theorem:

$\forall$ prime p

$\forall\ x \in \mathbb{Z}_p^* = \{1, \ldots, p-1\}$:

$$x^{p-1} = 1 \text{ in } \mathbb{Z}_p$$

Ex $p = 5$

$x = 2$

$$x^{p-1} = 2^4 = 16 = 1 \text{ in } \mathbb{Z}_5$$

$x = 3$

$$x^{p-1} = 81 = 1 \text{ in } \mathbb{Z}_5$$

Cor: Another way to find inverse mod p:

$x \in \mathbb{Z}_p^*$: $\quad x^{p-1} = 1$ in $\mathbb{Z}_p$

$x \cdot x^{p-2} = 1$ in $\mathbb{Z}_p$

$y = x^{p-2}$: $\quad x \cdot y = 1$ in $\mathbb{Z}_p$

inverse of x

Euler's thm generalizes Fermat's thm from p to all N

Euler's φ function:

$\varphi(N) =$ # of invertible els in $\mathbb{Z}_N$

$= |\mathbb{Z}_N^*|$

$N = 12$, $\mathbb{Z}_N^* = \{1, 5, 7, 11\}$

$\varphi(12) = 4$

$N =$ prime $\quad \mathbb{Z}_N^* = \{1, 2, \ldots, N-1\}$

$\varphi(N) = N - 1$

Euler's thm: $\forall N, \forall x \in \mathbb{Z}_N^*$

$$x^{\varphi(N)} = 1 \quad \text{in } \mathbb{Z}_N$$

Euler's thm: $\forall N, \forall x \in \mathbb{Z}_N^*$

$$x^{\varphi(N)} = 1 \quad \text{in } \mathbb{Z}_N$$

$N=12 \quad \varphi(N) = |\{1, 5, 7, 11\}| = 4$

$x = 5$

$$x^{\varphi(N)} = 5^4 = 625 = 1 \quad \text{in } \mathbb{Z}_N$$

$N = \text{prime} \quad \varphi(N) = |\{1, 2, \ldots, N-1\}| = N-1$

$$x^{\varphi(N)} = \underline{x^{N-1} = 1} \quad \text{in } \mathbb{Z}_N$$

|||

Fermat's Theorem

Easy & Hard Problems

x, y are n-bit long integers:

Easy:

- $x+y$
- $x-y$
- $x \cdot y$
- $GCD(x,y)$
- Modular inv: given x, find y s.t. $xy=1$ in $\mathbb{Z}_N$
- Modular exponentiation $\boxed{x^y}$

  by Euler's thm, wlog assume that $y < \varphi(N) < N$

  Ex: $y = 2\varphi(N)+5$

  $x^y = x^{2\varphi(N)+5} =$
  $= (x^{\varphi(N)})^2 \cdot x^5 = 1^2 \cdot x^5 = x^5$
- Check if N is prime

Hard:

- Factor N

  Even if $N = p \cdot q$, p, q are 1024-bit long primes. It's hard to find p or q.
- Given x, given y: $x^{1/y}$ modulo N

  $\parallel\!\mid$

  number z s.t. $z^y = x$

RSA

Rivest Shamir Adleman

Text Book RSA

Alice

- $N = p \cdot q$

  p, q - primes, 1024-bits long

- $e \cdot d = 1 \mod \varphi(N)$

- $pk = (N, e)$ encryption

- $sk = (N, d)$ decryption

- $N = p \cdot q$

  p, q - primes, 1024-bits long

- $\boxed{e \cdot d = 1}$ mod $\varphi(N)$

- $pk = (N, e)$ encryption

- $sk = (N, d)$ decryption

$m \in \mathbb{Z}_N^*$

$c = Enc(pk, m) = Enc(N, e, m) =$

$= \boxed{m^e}$ in $\mathbb{Z}_N$

Easy problem, I can do this efficiently

$Dec(sk, c) = Dec(N, d, m^e) =$

$= \boxed{(m^e)^d}$ in $\mathbb{Z}_N$ Easy problem.

Correct:

Bob: $m \longrightarrow m^e$

Alice $(m^e)^d = m^{e \cdot d}$

$e \cdot d = 1 \mod \varphi(N)$

$e \cdot d = k \cdot \varphi(N) + 1$:

$m^{ed} = m^{k \cdot \varphi(N) + 1} =$

$= \left(m^{\varphi(N)}\right)^k \cdot m$

$= 1^k \cdot m$

$= m$ in $\mathbb{Z}_N$

Secure: hard to decode without d

in order to decrypt :

$m^e \longrightarrow m$

compute e^{th} root of $m^e \mod N$