Tutorial V

06 November 2020 11:11

Assymetric Cryptography

- Basics of number theory
- RSA encryption
- Diffie Hellman key exchange
- Knapsack Cryptosystem

Basic Number theory

$\mathbb{Z}_n$ ⇝ set of all remainders after division by n

+ mod n , $(\mathbb{Z}_n, +)$ is a group

$\mathbb{Z}_n^*$ ⇝ multiplicative group mod n

⇝ for prime n $(\mathbb{Z}_n \setminus \{0\}, \cdot \bmod n)$

⇝ generally only elements with $\gcd(a,n) = 1$ with multiplication

---

$\frac{a}{b} \bmod n = a \cdot b^{-1} \bmod n$ (b^{-1} exists iff $\gcd(b,n)=1$)

~~$\frac{5}{3} \bmod 7 \neq 1{,}666$~~ ← INCORRECT

$5 \cdot 3^{-1} \bmod 7$ ($3^{-1} = 5$, $3 \cdot 5 = 15 \equiv 1 \bmod 7$)

$5 \cdot 5 \bmod 7$

$4 \bmod 7$

How to calculate inverses mod n?

Euclid's algorithm → algorithm to calculate $\gcd(a,b)$ for any $(a,b) \in \mathbb{Z}$

Bézout's identity → for a,b: $\gcd(a,b) = 1$ $\exists x,y$ s.t. $ax + by = 1$

Extended Euclid's algorithm → algorithm to calculate x,y from Bézout's identity

Extended Euclid's algorithm → algorithm to calculate x, y from Bézout's identity

$ax + by = 1$

$ax = 1 - by \quad | \bmod b$

$ax \equiv 1 \quad | \bmod b$

$a^{-1} \equiv x \quad \bmod b$

$ax \equiv 1 - 0$

Find $\gcd(17, 3) = 1$ (a = 17, b = 3)

$17 : 3 = 5 \quad rm\ 2$ → $2 = 17 - 3 \cdot 5$

$3 : 2 = 1 \quad rm\ 1$ ← last non-zero remainder is $\gcd(a, b)$ (17, 3)

→ $1 = 3 - 2 \cdot 1$

$2 : 1 = 2 \quad rm\ 0$

$1 = 3 - \boxed{2} \cdot 1$

$1 = 3 - (17 - 3 \cdot 5) \cdot 1$

$1 = 3 - 17 + 3 \cdot 5$

$1 = 3 \cdot 6 - 17 \cdot 1$ (b = 3, y = 6, a = 17, x)

$y = 6$

$x = -1$

$3^{-1} = 6 \quad \bmod 17 \qquad 3 \cdot 6 = 18 \equiv 1 \bmod 17$

$17^{-1} = 2 \quad \bmod 3 \qquad 2 \cdot 17 = 34 \equiv 1 \bmod 3$

Modular exponentiation

$a^b \bmod n$

$2^{303} \bmod 3$

~~$2^{303 \bmod 3} = 2^0 = 1 \bmod 3$~~ ← INCORRECT

$2^{303} = 2^{303 \bmod 2} = 2^1 = 2 \bmod 3$

Euler's Totient theorem

for a, n: $a < n$, $\gcd(a, n) = 1$

$a^{\phi(n)} \equiv 1 \bmod n$

$\varphi(n)$ – Euler's theta function

– Euler's totient function

= number of $a < n$, $\gcd(a, n) = 1$

$\phi(p) = p - 1$ for prime p

$$2^{303} = 2^{303 \bmod 2} = 2^1 = 2 \bmod 3$$

For a, with $\gcd(a,n) = 1$

$$a^b \bmod n = a^{b \bmod \varphi(n)} \bmod n$$

$$\underbrace{\overbrace{a \cdot a \cdot a \cdot a \cdot}^{\varphi(n)=1} \overbrace{\cdot \; \cdot \; \cdot}^{\varphi(n)=1} \cdots \overbrace{a}^{b \bmod \varphi(n)}}_{b\text{- times}}$$

$\varphi(p) = p-1$ for prime p

$$\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n) \cdot \frac{d}{\varphi(d)}$$

where $\gcd(m,n) = d$

p, q are prime

$$\varphi(p \cdot q) = \varphi(p) \cdot \varphi(q) \cdot \frac{1}{\varphi(1)} = (p-1)(q-1)$$

For prime n you recover Fermat's little theorem

$\forall\, a < n$ $\quad \varphi(n)$

$$a^{n-1} \equiv 1 \mod n$$

$$a^{b \bmod n-1} \mod n$$

Important problems in assymetric cryptography

Factorization easy: Given a, b find c, s.t. $c = a \cdot b$

hard: Given c find a, b, s.t. $c = a \cdot b$

Essentially trying all divisors between 2 and $\sqrt{c}$ is the best algorithm we know.

$\boxed{2048\text{- bits}}$ $\quad c \,\hat{=}\, 2^{2048}$ $\quad \boxed{\sqrt{c} = 2^{1024}}$

Number of protons in the Universe $\approx 2^{300}$

Discrete logarithm problem easy: given a, b and n calculate $a^b \bmod n$

hard: given c, a, n calculate b, such that $c = a^b \bmod n$ $\;$ $b \in \{1, .., \varphi(n)\}$

$b = \log_a c \bmod n$ $\quad$ if $\gcd(a,n) = 1$

RSA encryption

Private: $p, q \to$ two large primes $\quad n = p \cdot q$

$d = e^{-1} \bmod \bmod \underbrace{(p-1)(q-1)}_{\varphi(n)}$

$\boxed{\textbf{Public: } e, n}$

Encryption of message $w < n$ $\quad$ if w is larger, this needs to be done in blocks

$\boxed{172}\boxed{419}$ $\quad 1000 < n < 9999$

$$C = w^e \bmod n$$

Decryption of ciphertext c

$$w = c^d \bmod n$$
$$= (w^e)^d \bmod n$$
$$= w^{e \cdot d} \bmod n$$
$$= w^{e \cdot d \bmod \varphi(n)} \bmod n$$
$$= w^1 \bmod n$$

! $\gcd(w, n) = 1$

What can an adversary do if they do not know p, q, d ?

1.) Factorize $n \Rightarrow p$ and $q \Rightarrow \varphi(n) = (p-1)(q-1) \Rightarrow$ calculate $d = e^{-1} \bmod n$

Hard

efficient

2.) Can I find an algorithm to calculate $\varphi(n)$ without factoring n?

Then we can factor n like this

$$\left.\begin{array}{l} p \cdot q = n \\ (p-1) \cdot (q-1) = \varphi(n) \end{array}\right| \to \text{easy to solve system of equations}$$

3.) $e, n \to d$ $\quad$ RSA problem

This is hard (we do not know an efficient algorithm)
but probably (we do not know an efficient reduction)
not as hard as factoring.

Other RSA weaknesses

For known (w, c) pairs or $w^e = c \mod n$ you can find other pairs

(w^2, c^2) is also a valid pair

$$(w^2)^e \equiv w^{2e} = w^e \cdot w^e = c \cdot c = c^2 \mod n$$

Whenever you see c^2 in a channel and you know (w, c) is a valid pair you also know that c^2 decrypts as w^2.

(w^n, c^n) is a valid pair for any c.

if (w_1, c_1) and (w_2, c_2) are two valid pairs then also

$(w_1 \cdot w_2, c_1 c_2)$ is a valid pair

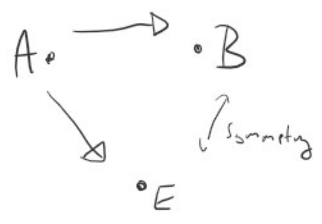
$$(w_1 \cdot w_2)^e = w_1^e \cdot w_2^e = c_1 \cdot c_2 \mod n$$

TEXT → ASCII

i	E	S
16-bit	16-bits	16-bit
RSA(i)	RSA(E)	RSA(S)

THIS IS JUST A MONOALPHABETIC SUBSTITUTION (NOT SECURE)

DIFFIE-HELLMAN KEY DISTRIBUTION



Prerequisities

p - is a large prime

$\boxed{q \in \mathbb{Z}_p^* \text{ with a large order}}$

$a^{p-1} = 1 \mod p$

$1 \quad 1^2 \quad 1^3$ — order $(1) = 1$

$1 \quad 1 \quad 1$

$(p-1)^1 \ (p-1)^2 \ (p-1)^3$ — order $(p-1) = 2$

$p-1 \quad 1 \quad p-1$

$A \to B$

$A = q^x \mod p$ — these are chosen randomly

$B \to A$

$B = q^y \mod p$

A calculates

A calculates

$k = B^x \bmod p = g^{xy} \bmod p$

B calculates

$k = A^y \bmod p = g^{yx} \bmod p$

$p-1 \quad 1 \quad p-1$

$\log_{p-1} c \bmod n$

What can the adversary do?

1.) calculate $x = \log_g A \bmod p$, $y = \log_g B \bmod p$ → Discrete logarithm problem HARD

$k = g^{xy} \bmod p$

2.) given g^x and g^y calculate $g^{xy} \bmod p$

$\boxed{\text{DH 1}}$ → believed to be hard

KNAPSACK CRYPTOSYSTEM

NP-Complete problem (based on)

given $(x_1, \dots, x_n)$ $x_i \in \mathbb{Z}_m$ for large n

and a constant c

find $b \in \{0,1\}^n$, such that

$\vec{x} \cdot \vec{b} = c \mod m$

Easy instance - superincreasing vectors

X is superincreasing $\forall i \ x_i > \sum_{j<i} x_j$

$x_2 > x_1$
$x_3 > x_1 + x_2$
$x_4 > x_1 + x_2 + x_3$

for $c < 2x_n$

an instance with superincreasing X and c is easy.

Public information X, m $\quad m > 2x_n > \sum_i x_i$

Private information u invertible mod m and $X' = u^{-1} \cdot X \bmod m$ where X' is superincreasing encryption

$w \in \{0,1\}^n$

$c = w \cdot X \mod m$

(c, X, m) - are a subsetsum instance

decryption calculate $u^{-1} \cdot c = c'$ mod p

then solve subsetsum instance with (c', x')

$c = w \cdot X \quad / u^{-1}$

$c u^{-1} = w \cdot u^{-1} \cdot X \mod m$

$c' = w \cdot x'$

$X' = (1, 3, 7, 13, 29, 59, 127)$

$X = 155 \cdot X' \mod 257$

$\quad\; u \qquad\qquad\quad m$

$= (155, 208, 57, 216, 126, 150, 153)$

$w = (0111011)$

$c = w \cdot X = 208 + 57 + 216 + 150 + 153 = 784 \mod 257$

$= 13 \mod 257$

$13, X$

$13 \cdot u^{-1} = 13 \cdot 155^{-1} \mod 257$

$= 13 \cdot 194 \mod 257$

$= 1950 + 600 - 18 = 2522 \mod 257$

$= -48 \mod 257$

$= 209 \mod 257$

$(209, x')$

$(0\ 1\ 1\ 1\ 0\ 1\ 1) = w$

$X' = (1, 3, 7, 13, 29, 59, 127)$

$209 - 127 = 82$

$82 - 59 = 23$

$23 - 13 = 10$