Reference

Thursday, April 18, 2024 11:47 AM

1. "An Introduction to Mathematical Cryptography" by Hoffstein, Pipher and Silverman
2. Dan Boneh Cryptography course on Coursera

Some math background

Tuesday, April 16, 2024 6:09 PM

$\mathbb{Z}/m\mathbb{Z} = \{0, 1, \dots, m-1\}$ ring of integers modulo m.

Binary operations: $+$ and $\cdot$ $\rightarrow$ $(\mathbb{Z}/m\mathbb{Z}, +)$, $(\mathbb{Z}/m\mathbb{Z}, \cdot)$

notation: $\mathbb{Z}_m \leftrightarrow \mathbb{Z}/m\mathbb{Z}$ quotient ring of $\mathbb{Z}$ by principal ideal $m\mathbb{Z}$

Example: $\mathbb{Z}/5\mathbb{Z}$ is just $\mathbb{Z}_5$.

$\{0, 1, 2, 3, 4\}$ you can do $2+3 = 5 = 0 \mod 5$

or $2 \cdot 3 = 6 = 1 \mod 5$

$(\mathbb{Z}/m\mathbb{Z})^* = \{a \in \mathbb{Z}/m\mathbb{Z} : \gcd(a, m) = 1\}$

$= \{a \in \mathbb{Z}/m\mathbb{Z} : a \text{ has an inverse modulo } m\}$

Numbers that have inverses are called **units**.

$(\mathbb{Z}/m\mathbb{Z})^*$ is just the set of all units, called **group of units modulo m**.

Example: $\mathbb{Z}/24\mathbb{Z} = \{0, 1, 2, \dots 23\}$

$(\mathbb{Z}/24\mathbb{Z})^* = \{1, 5, 7, 13, 17, 19, 23\}$

$\mathbb{Z}/7\mathbb{Z} = \{0, 1, 2, \dots 6\}$

$(\mathbb{Z}/7\mathbb{Z})^* = \{1, 2, \dots, 6\}$

When m is prime (Z/pZ case), all elements other than 0 are units.

If p is prime, then the set $\mathbb{Z}/p\mathbb{Z} = \{0, 1, \dots, p-1\}$ is a finite field, also denoted as $\mathbb{F}_p$.

Also, $(\mathbb{Z}/p\mathbb{Z})^* = \{1, 2, \dots p-1\}$ is often denoted as $\mathbb{F}_p^*$ it is just all the non-zero

Also, $(\mathbb{Z}/p\mathbb{Z})^*$ $\{1, 2, \ldots p-1\}$ is often denoted as $\mathbb{F}_p^*$, it is just all the non-zero elements in the finite field.

Fermat's Little Theorem

Let p be a prime, then $\forall x \in (\mathbb{Z}/p\mathbb{Z})^*$:

$$x^{p-1} = 1 \bmod p$$

Example: $p = 5$, $3^4 = 81 = 1 \bmod 5$

Fermat's Little Theorem can help with modular inverse computation in Z/pZ

Pick $x \in (\mathbb{Z}/p\mathbb{Z})^*$

$\Rightarrow$ $x^{p-1} = 1 \bmod p$

$\Rightarrow$ $x \cdot x^{p-2} = 1 \bmod p$

$\Rightarrow$ $x^{-1} = x^{p-2} \bmod p$ (less efficient than Euclid)

Fermat's Little Theorem can help with random prime generation

Want to generate a large random prime p with length 1024 bits

Step 1: choose random integer $p \in [2^{1024}, 2^{1025} - 1]$

Step 2: test if $2^{p-1} = 1 \bmod p$

If yes, return p; otherwise, repeat.

Probability of getting false positive is negligible.

The structure of $(\mathbb{Z}/p\mathbb{Z})^*$

Theorem (Euler): $(\mathbb{Z}/p\mathbb{Z})^*$ is a cyclic group, that is

$$\exists\, g \in (\mathbb{Z}/p\mathbb{Z})^* \text{ s.t. } \{1, g, g^2, \cdots, g^{p-2}\} = (\mathbb{Z}/p\mathbb{Z})^*$$

(g^{p-1} by Fermat)

g is called a generator of $(\mathbb{Z}/p\mathbb{Z})^*$.

Example: $p=7$. $\{1, 3^1, 3^2, 3^3, 3^4, 3^5\} = (\mathbb{Z}/7\mathbb{Z})^*$, $g=3$

$1\ 3\ 2\ 6\ 4\ 5 \mod 7$

Not every element is a generator: $\{1, 2^1, 2^2, 2^3, 2^4, 2^5\} = \{1, 2, 4\}$

$1\ 2\ 4\ 1\ 2\ 4 \mod 7$

Euler's phi function (totient function)

$$\phi(m) = \#(\mathbb{Z}/m\mathbb{Z})^* = \#\{0 \le a < m : \gcd(a, m) = 1\}$$

($\#(\mathbb{Z}/m\mathbb{Z})^*$: size of $(\mathbb{Z}/m\mathbb{Z})^*$)

"#" is "number of"

Example: $\phi(24) = 8$ $\quad \phi(7) = 6 = 7-1$

$\phi(p) = p-1$ in general

Computation:

1. p prime, a positive integer,
then $\phi(p^a) = p^a - p^{a-1} = p^a(p-1)$

2. If a, b coprime, then $\phi(ab) = \phi(a)\phi(b)$

3. n positive integer, prime factorization $p_1^{e_1} \cdots p_k^{e_k}$ (fundamental theorem of arithmetic)
then $\phi(n) = (p_1^{e_1} - p_1^{e_1-1}) \cdots (p_k^{e_k} - p_k^{e_k-1})$

3. n positive integer, prime factorization $p_1^{e_1} \cdots p_k^{e_k}$

then $\phi(n) = (p_1^{e_1} - p_1^{e_1-1}) \cdots (p_k^{e_k} - p_k^{e_k-1})$

$$= p_1^{e_1}\left(1 - \frac{1}{p_1}\right) \cdots p_k^{e_k}\left(1 - \frac{1}{p_k}\right)$$

$$= (p_1^{e_1} \cdots p_k^{e_k})\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right)$$

$$= n \cdot \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right)$$

Theorem (Euler): $\forall x \in (\mathbb{Z}/N\mathbb{Z})^* : x^{\phi(N)} = 1 \bmod N$

Example: $5^{\phi(12)} : 5^4 = 625 = 1 \bmod 12$

Diffie-Hellman Key Exchange

Tuesday, April 16, 2024 6:08 PM

Diffie-Hellman Key Exchange protocol was designed to exchange secret key over insecure channel. After that Alice and Bob do traditional symmetric crypto -> "hybrid encryption

Keygen A trusted 3rd party publishes a large prime p and an integer g having prime order in $\mathbb{F}_p^*$.

↑ non-zero elements in $\mathbb{F}_p$

Private computation

Alice

Pick secret a

Compute $A = g^a \bmod p$

Bob

Pick secret b

Compute $B = g^b \bmod p$

Public exchange

A →

← B

Private computation

Compute $B^a \bmod p$

Compute $A^b \bmod p$

Correctness: $B^a = (g^b)^a = g^{ba} = g^{ab} = (g^a)^b = A^b \bmod p$

Diffie-Hellman Problem (DHP)

Let p be a prime number and g an integer. The Diffie-Hellman Problem is the problem of computing the value of g^ab mod p from the known values of g^a mod p and g^b mod p.

Alice Eve Bob

$A = g^a \bmod p$ — (A) → $B = g^b \bmod p$

← (B)

Eve knows A and B.

Eve knows A and B,
but not the shared secret

The difficulty relies on the hardness of discrete log problem.

Eve: solve $g^a \bmod p$ or $g^b \bmod p$ to get a or b
then compute $B^a \bmod p$ or $A^b \bmod p$.

Fermat's Little Theorem:

$a^{p-1} = 1 \bmod p$ if $p \nmid a$ ($p \mid a$ then $a = 0 \bmod p$ $\Rightarrow a^{p-1} = 0 \bmod p$)

Is this theorem for non-prime m in general? No

But, we can generalize it to $m = pq$ where p, q are distinct primes.

Observation: $m = 15 = 3 \cdot 5$

$a^4 = 1 \bmod 15$ for $a = 1, 2, 4, 7, 8, 11, 13$ and 14 ← $\gcd(a, 15) = 1$

$a^4 \neq 1 \bmod 15$ for $a = 3, 5, 6, 9, 10,$ and 12 ← $\gcd(a, 15) \neq 1$

$a^4 = 1 \bmod 15 \longrightarrow$ (equivalent) $a^4 = 1 \bmod 3$ and $a^4 = 1 \bmod 5$

$\Rightarrow 15 \mid a^4 - 1$ $\Rightarrow 3 \mid a^4 - 1$ $\Rightarrow 5 \mid a^4 - 1$

$\Rightarrow 15 \mid a^4 - 1$

verify if ① $a^4 = 1 \bmod 3$ and ② $a^4 = 1 \bmod 5$ hold:

① $a^4 = (a^2)^2 = (a^{3-1})^2 = 1^2 = 1 \bmod 3$ by Fermat

② $a^4 = a^{5-1} = 1 \bmod 3$ By Fermat

You can see 4 is special in this case: ① it is multiple of $p-1$ for $p = 3$
② it is multiple of $p-1$ for $p = 5$

In general:

In general:

Theorem: (Euler's formula for pq)

Let p, q be distinct primes and $g = \gcd(p-1, q-1)$

Then

$$a^{\frac{(p-1)(q-1)}{g}} = 1 \bmod pq \qquad \text{for all } a \text{ s.t. } \gcd(a, pq) = 1$$

If p and q are odd primes (not 2), then:

$$a^{\frac{(p-1)(q-1)}{2}} = 1 \bmod pq \qquad \text{for all } a \text{ s.t. } \gcd(a, pq) = 1$$

This theorem is a generalization of Fermat's little theorem, and it will be used in the proofs of the next two propositions.

Security of RSA relies on solving $\boxed{x^e = c \bmod N}$

In other words, it is hard to take eth root modulo N.

If N is prime, it is easy to compute eth root modulo N.

Proposition: Let p be prime, $e \geq 1$ integer s.t. $\gcd(e, p-1) = 1$.

(e has inverse mod $p-1$; $de = 1 \bmod p-1$)

Then the congruence $x^e = c \bmod p$ has unique solution $x = c^d \bmod p$

If $N = pq$ but attack can factor N, then RSA is broken.

Because attacker knows p and q, can compute $\phi(N) = (p-1)(q-1)$,

then compute d s.t. $de \equiv 1 \bmod (p-1)(q-1)$, then learns $x = c^d \bmod pq$.

Proposition: Let p, q be distinct primes, $e \geq 1$ s.t. $\gcd(e, (p-1)(q-1)) = 1$.

(e has inverse mod $(p-1)(q-1)$: $de = 1 \bmod (p-1)(q-1)$)

Then the congruence $x^e = c \bmod pq$ has unique solution $x = c^d \bmod pq$

↑

Correctness of RSA decryption

RSA

	Alice	Bob
key gen		Choose secret primes p and q choose encryption exponent e with $\gcd(e,(p-1)(q-1)) = 1$. Publish $N = pq$ and e. ($p, q \approx \sqrt{N}$) (N, e) is Bob's public key pair.
Encryption	Choose plaintext m. Use Bob's public key (N, e) to compute $c = m^e \bmod N$ Send ciphertext c to Bob.	
Decryption		use his (p,q) Compute d s.t. $ed = 1 \bmod (p-1)(q-1)$ Compute $m' = c^d \bmod N = m$.

Security analysis

Setup: p, q prime, $N = pq$, e, c integers

Problem: Solve congruence $x^e = c \bmod N$ for variable in x.

(In PHP, it was solving a in $g^a \bmod p$)

Easy Bob knows p and q, can easily solve for x — pair

p and q: trapdoor info

Hard Eve, who does not know p and q, can't solve for x

$\Rightarrow$ RSA encryption is a trapdoor function

Some further discussions

Some further discussions

$N \rightarrow$ modulus
$e \rightarrow$ encryption exponent
$d \rightarrow$ decryption exponent

1. choice of e

$e = 1 \Rightarrow c = m$, RSA broken

$e = 2 \Rightarrow \gcd(e, (p-1)(q-1)) \neq 1$, does not work

$e = 3 \Rightarrow$ fine, but some people worry about security

$\boxed{e = 2^{16} + 1 = 65537}$

fast and secure

2. Eve can break RSA if she knows $p+q$

Why? $de = 1 \bmod (p-1)(q-1)$

$$(p-1)(q-1) = pq - p - q + 1$$

$$= pq - (p+q) + 1$$

$$= N - (p+q) + 1$$

$\uparrow$ public

And in fact, knowing $p+q$ is equivalent to knowing p and q in RSA. Consider the polynomial:

$$X^2 - (p+q)X + pq$$

roots are: $X = \dfrac{(p+q) \pm \sqrt{(p+q)^2 - 4pq}}{2}$ $\left(x = \dfrac{-b \pm \sqrt{b^2 - 4ac}}{2a} \right)$

$$X = \frac{(p+q) \pm \sqrt{(p+q)^2 - 4N}}{2}$$

Since the polynomial can be factored into $(X-p)(X-q)$:

$$p = \frac{(p+q) + \sqrt{(p+q)^2 - 4N}}{2}$$

$$p = \frac{(p+q) + \sqrt{(p+q)^2 - 4N}}{2}$$

$$q = \frac{(p+q) - \sqrt{(p+q)^2 - 4N}}{2}, \quad \text{or swap}$$

3. Eve's job is to solve x th $x^e = c \bmod N$, not factor N. Factoring N is just one way of breaking RSA. If Eve knows how to compute eth root modulo N, she can decrypt messages without knowing $\phi(pq) = (p-1)(q-1)$. No algorithm can do this efficiently at this moment.

Further research

Thursday, April 18, 2024 12:00 PM

Number Theory notes by Ben Lynn: https://crypto.stanford.edu/pbc/notes/numbertheory/

A paper on RSA attacks by Dan Boneh: https://crypto.stanford.edu/~dabo/papers/RSA-survey.pdf

Solve challenges on https://cryptohack.org/challenges/, specifically, challenges in "RSA" and "Diffie-Hellman" categories. You probably want to research "lattice-based cryptography" for more sophisticated attacks on RSA.