Math Primer to Understand RSA Cryptographic Primitives

October 30, 2018

Abstract

In order to understand RSA Cryptographic Primitives, we must have knowledge on modular arithmetic, finding inverse of a given number. In this article I explain basic operations in modular arithmetic, Euclidean algorithm to find gcd of two positive integers, Extended Euclidean algorithm to find inverse of a given number.

1 Modular Arithmatic

In modulo aruthmatic we have a modulo operator denoted by 'mod'. For example: 7 (mod 2) = 1, which means when 7 divided by 2 gives remainder 1.

1.1 Different operations in modulo arithmatic:

1.1.1 Addition:

For example:

- 2+1 (mod 5) = 3 (mod 5)
- 2+3 (mod 5) = 5 (mod 5) =0 (mod 5)
- 2+10 (mod 5) = 12 (mod 5) = 2 (mod 5)

1.1.2 Subtraction:

For example:

- 2-1 (mod 5) = 1 (mod 5)
- 2-3 (mod 5) = -1 (mod 5) = 4 (mod 5) In the above example -1 can be written as 4(i.e -1+5 = 4). $\{-6, -1, 4, 9, 14\}$ In this group any element can be replaced by other element. Each element is generated by adding 5 to the previous element.

1.1.3 Multiplication:

For example:

- $4 * 5(mod 5)$ = 20 (mod 5) = 0 (mod 5)
- $(2+3)*7$ (mod 5) = $5*2$ (mod 5) =0 (mod 5) Here, for easy calculation 7 can be written as 2 (i.e 7-5=2).

1.1.4 Division:

$\frac{a}{b}$(mod c) = $a * b^{-1}$(mod c).
In order to calculate b^{-1}, it needs to satisfy the condition that gcd(b,c)=1 then b^{-1} exists.

2 Euclidean algorithm to find gcd of two positive integers

Ex: gcd(160, 28)

$160 = 5 * 28 + 20$ (Divide 160 by 28, gives remainder 20)

$28 = 1*20+8$ (Divide 28 by above equation remainder 20, gives remainder value 8)

$20 = 2 * 8 + 4$ (Divide 20 by above equation remainder 8, gives remainder value 4)

$8 = 2 * 4 + 0$ (Divide 8 by above equation remainder 4, gives remainder value 0)
In the final equation when $8 \div 4$ gives remainder 0.So gcd(160, 28) = 4.

3 To find b^{-1} (mod c)

We need to find the value 'x' such that $b * x = 1$(mod c).
For example:

- 6^{-1} (mod 7).

  gcd(6, 7) = 1 .

  so 6^{-1} exists. In order to find 6^{-1}, multiply 6 with $1, 2, 3, 4, 5, 6$ (i.e given mod value is 7, so you could multiply 6 with integers from 1 to 6. If given mod value is 9 then you could multiply 6 with integers from 1 to 8).

  $6 * 1$= 6(mod 7)

  $6 * 2$= 12(mod 7)= 5 (mod 7)

$6*3$= 18(mod 7)= 4 (mod 7)

$6*4$= 24(mod 7)= 3 (mod 7)

$6*5$= 30(mod 7)= 2 (mod 7)

$6*6$= 36(mod 7)= 1 (mod 7)

6^{-1}(mod 7)= 6(mod 7).

- 0^{-1}(mod 7) does not exist.

3.1 Extended Euclidean algorithm to find inverse:

Ex: Find 7^{-1}(mod 19).

Step 1:

$19 = 2*7+5 \rightarrow (3)$

$7 = 1*5+2 \rightarrow (2)$

$5 = 2*2+1 \rightarrow (1)$

$2 = 2*1+0$.

In the final equation when '2' is divided by '1' gives remainder '0'. So gcd(7,19)is 1 and 7^{-1}(mod 19) exist.

Step 2:

Equation(1) can be rearranged as

$1 = 5 - 2*2$

$= 5 - 2(7 - (1*5)) \rightarrow$ from (2)

$= 5 - 2*7 + 2*5 = 3*5 - 2*7$

$= 3(19 - (2*7)) - 2*7 \rightarrow$ from (3)

$= 3*19 - 8*7 \rightarrow$(4).

Take (mod 19) on both sides of equation (4), we get

$1(mod19) = -7*8(mod19))$

$7^{-1}(mod19) = -8(mod19) = 11(mod19)$.

Relatively prime numbers :

Two integers are said to be relatively prime to each other if their gcd is one. Let a,b belongs to the set of prime integers. If gcd(a,b)=1 then a,b are relatively prime to each other.

4 Number sets notations :

- $\mathbb{P}$ represents set of prime numbers, where $\mathbb{P} = \{2, 3, 5, 7...\}$.
- $\mathbb{W}$ represents set of whole numbers, where $\mathbb{W} = \{0, 1, 2, 3...\}$.
- $\mathbb{N}$ represents set of natural numbers, where $\mathbb{N} = \{1, 2, 3, 4...\}$. It is also denoted by $\mathbb{Z}^+$.
- $\mathbb{Z}$ represents set of integers, where $\mathbb{Z} = \{... - 4, -3, -2, -1, 0, 1, 2, 3, 4...\}$.
- Irrational number is a real number but it can not be represented as a fraction. $\mathbb{I}$ represents set of irrational numbers, Ex:π=3.14159....
- Rational number is a real number that can be represented as a fraction. $\mathbb{Q}$ represents set of rational numbers. Ex:0.3333=$\frac{1}{3}$, 0.2=$\frac{1}{5}$.
- Real numebrs include set of integers, set of rational and set of irrational numbers. $\mathbb{R}$ represents set of real numbers.
- Complex number is a number that can be represented in a+ib form.$\mathbb{C}$ represents set of complex numbers. where $\mathbb{C} = \{3 + i2, i10, 1 - i...\}$.

5 Euler's PHI function or Euler's totient function:

Let $n \in \mathbb{Z}^+$.

The Euler's phi function,

$\Phi(n)$ = number of positive integers, not greater than n, that are relatively prime to n.

Ex: find $\Phi(7)$

gcd(1,7)=1 ;gcd(2,7)=1 ;gcd(3,7)=1 ;gcd(4,7)=1; gcd(5,7)=1 ;gcd(6,7)=1; gcd(7,7)=7.

Therefore Φ(7)=6.

5.0.1 Useful formulas to calculate $\Phi(n)$:

- If n is a prime number then $\Phi(n) = n - 1$.
- If n is a prime number, k= 1, 2, 3...then $\Phi(n^k) = n^k - n^{(k-1)}$.
- If n belongs to the set of positive integers except '1', then $n = p_1^{\alpha_1}.p_2^{\alpha_2}.....p_m^{\alpha_m}$. Where p_i's are prime numbers.

  $\alpha_i \in$ set of positive integers, $1 \leqslant i \leqslant m$ then

  $\Phi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2})...(1 - \frac{1}{p_m})$.
- m,n$\in$ set of positive integers, gcd(m,n)=1 then $\Phi(mn) = \Phi(m).\Phi(n)$.

Example: 1. Find $\Phi(6)$.

Sol) Let n= $6 = 3 * 2$.

$\Phi(6) = \Phi(3 * 2) = \Phi(3) * \Phi(2) = (3 - 1) * (2 - 1) = 2$.

Example: 2. Find $\Phi(120)$.

Sol) Let n= $120 = 2^3.3.5$.

$\Phi(120) = \Phi(2^3.3.5) = 120 * (1 - \frac{1}{2}) * (1 - \frac{1}{3}) * (1 - \frac{1}{5}) = 120 * \frac{1}{2} * \frac{2}{3} * \frac{4}{5} = 32$.

- Let p and q are two co-prime numbers. If x=a (mod p) and x=a (mod q), then x= a (mod pq).

  Example: if 17 = 2 (mod 5), 17= 2 (mod 3) then 17 = 2 (mod 15).

5.1 Fermat's little theorem :

- 'p' is a prime number, $a \in \mathbb{Z}^+$ and $p \nmid a$ (where 'a' is not divisible by 'p'). Then $a^{p-1} \equiv 1$(mod p) .
- 'p' is a prime number, $a \in \mathbb{W}$ then $a^p \equiv$ a (mod p) .

5.2 Euler's theorem or Euler - Fermat's theorem(EFT)

EFT states that if integers a, n are relatively prime (i.e gcd(a,n)=1) then $a^{\Phi(n)}=$ 1 (mod n).