Mathematical tools used for cryptography

Cryptography is based on some areas of mathematics. Various types of mathematical concepts are used in cryptography for the encipherment of data. Here we are going to discuss on some of these mathematical concept such as,

- Integer arithmetic
- Modular arithmetic
- Matrices
- Linear Congruence

- **Integer arithmetic:**
  In this type, a set of integer numbers and some operations are used. In cryptography this integer operations are used as the background of modular operations discussed subsequently.

  Integer set:
  In mathematic the set of all integers are denoted by the letter **Z.** This set contains all the integral numbers from negative infinity to positive infinity.

  Z= {…,-3,-2,-1,0,1,2,3…}

  Binary Operations:
  Binary operations are those which takes two numbers as input and produces one number as output. In cryptography three common type of binary operations on integers are used, Additions, Subtraction, and Multiplication.

  6+(-3)=3
  34-20=14
  (-3)×(-4)=12

  Integer Division:
  In integer division if ***a*** is divided by ***n*** then it produced two integer ***q*** and ***r*** we can write this relation between four integer as

  $$a = q \times n + r$$

  Assuming two restriction first one is ***n is a positive integer(n>0)*** and another one is ***r be a non-negative integer(r>=0).***

  Divisibility:
  In cryptography Divisibility is commonly used. In the above relation if a is a non zero value and $r = 0$ the the relation reduced to

  $$a = q \times n$$

  We can say that a is divisible by n if the r is not equal to zero and if the $r = 0$ then we can say that a is not divisible by n. we can write the divisibility as $a|n$

  4 divide 32 as 32=8×4 we can denote it as 4|32

Properties of divisibility:

If $a|1$, then $a = \pm 1$
If $a|b$ and $b|a$ then $a = \pm b$
If $a|b$ and $b|c$ then $a|c$
If $a|b$ and $a|c$ then $a|(m \times b + n \times c)$, m and n are arbitrary integers.

For a positive integer there can have more than one divisor. There are two important points to remember on divisor,
1 has only one divisor that is 1.
All positive integers have at least two positive divisors 1 and itself.

Greatest common divisor (GCD:

Two positive integers can have one or more than one common divisor among them which is greatest is called Greatest Common Divisor (GCD) in cryptography there was many use of this GCD. i.e. **1,2,4** are the common divisor of the **12** and **140** among them **4** is the GCD of this two number.

Euclidean Algorithm:

Finding GCD of two integers by listing all the common divisor is not a practical way all the time. Euclidean algorithm can do this without listing all the common divisor. Euclidean algorithm is based on the following two facts.

GCD(a,0) = a
GCD(a,b) = GCD(b,r), r is the remainder of dividing a by b.

To calculate the GCD we can use the second case several times and the first fact once.
For example, to calculate the GCD of 36 and 10 we can use Euclidean method as follows,

GCD(36, 10)=GCD(10,6)=GCD(6,4)=GCD(2,0)=2

Algorithm(a,b)

```
{
    r1=a
    r2=b
    While(r2>0)
    {
        q=r1/r2
        r=r1-q×r2
        r1=r2
        r2=r
    }
    gcd=r
    return(gcd)
}
```

- **Modular arithmetic:**

In the division operation there are two input *a* and *b* and two output *q* and *r*. In modular arithmetic we can find only one of the two outputs, the remainder that is *r*. that is the value of r when we divide *a* by *n.*

Modulo Operator:

To calculate remainder from a division operation we us a binary operator called modulo operator and shown as ***mod.*** The second operand of mod is called modulus. The output r is called residue.

$r = a \bmod n$

For example,

$37 \bmod 5 = 2$
$36 \bmod 12 = 0$

Set of Residues (Z_n):

The result of modulo operation with modulus n is an integer between 0 and n-1. That is the result of *a mod n* is always a non negative integer less than n. Thus the modulus operation with n creates a set on n-1 elements called set of least residues modulo n or Z_n

For example the Set of Residues for modulus 2, 6 and 13 are

$Z_2 = \{0,1\}$
$Z_4 = \{0,1,2,3\}$
$Z_{13} = \{0,1,2,3,4,5,6,7,8,9,10,11,12\}$

Congruence:

The mapping from Z to Z_n is not one-to-one infinite member of Z can map to a single member of Z_n.

As Example $12 \bmod 10 = 2$,
$22 \bmod 10 = 2$,
$132 \bmod 10 = 2$ *and so on*

In the above example the value 12, 22 and 132 are called congruent of mod 10. The operator (≡) is used to represent congruence. The phrase (mod n) to the right side of the congruence is used to define the value of modulus for which the congruence relationship valid.

$2 \equiv 12 \pmod{10}$
$13 \equiv 23 \pmod{10}$
$8 \equiv 13 \pmod{5}$
$-8 \equiv 12 \pmod{10}$

Residue classes:

Residue classes *[a]* are the set of integers congruent modulo *n*. It is the set of all integer such that $x = a(mod\ n)$. For example if n is 5 we have 5 sets [0],[1],[2],[3],[4].

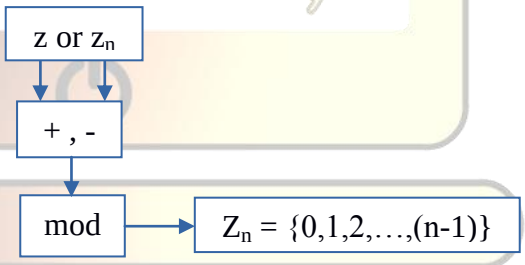
[0] = {…,-20,-15,-10,-5,0,5,10,15,20,...}
[1] = {…,-19,-14,-9,-4,1,6,11,16,21,...}
[2] = {…,-18,-13,-8,-3,2,7,12,17,22,...}
[3] = {…,-17,-12,-7,-2,3,8,13,18,23,...}
[4] = {…,-16,-11,-6,-1,4,9,14,19,24,...}

In each set of residue class of a integer there is a least non negative integer, a set consist of these least integers is called least residue modulo n denoted as Z_n.

For example The $Z_5 = \{0,1,2,3,4\}$

Operations on Z_n:

Three binary operation (addition, subtraction, multiplication) can be defined for the set Z_n as like we defined for Z. The result of the operations needs to be mapped to Z_n by applying mod operation with *n* on the result.



Properties:

In modular arithmetic there were the following properties,

1. $(a + b)\ mod\ n = [(a\ mod\ n) + (b\ mod\ n)]\ mod\ n$
2. $(a - b)\ mod\ n = [(a\ mod\ n) - (b\ mod\ n)]\ mod\ n$
3. $(a \times b)\ mod\ n = [(a\ mod\ n) \times (b\ mod\ n)]\ mod\ n$

Inverses:

In modular arithmetic we can find the inverse of a number relative to a particular operation, basically there are two kind of Inverse such as additive inverse relative to addition operation and multiplicative inverse relative to multiplication operation.

Additive Inverse:

In addition operation on Z_n two integer a and b are additive inverse of each other if,

$$a + b = 0(mod\ n)$$

The additive inverse can be calculated as $b = n - a$
For example the additive inverse of 2 in Z_{10} is 10-2=8 that means 2 and 8 are additive inverse of each other.

<u>In modular arithmetic each integer has an additive inverse the sum of the two additive inverse is congruent to 0 (mod n).</u>

Multiplicative Inverse:

In multiplication operation on Z_n two integer *a* and *b* are multiplicative inverse of each other if,

$$A * b = 1(mod\ n)$$

For example the multiplicative inverse of 7 in Z_{10} is 3, as (7*3) mod 10=1.

- ***<u>In modular arithmetic each integer may or may not have a multiplicative inverse, if it has, then the product of the two multiplicative inverse is congruent to 1 (mod n).</u>***
- ***<u>An integer a in Z_n has a multiplicative inverse if and only if GCD(n,a)=1 mod n</u>***

Addition and multiplication table in Z_n:

In the following figure we show two tables for addition and multiplication, in addition table each cross sectional cell contains the result of the addition operation followed by a mod operation. From this table we can find the inverse of the integers also. In the table when the result of the operation is Zero it implies that the corresponding integers are additive inverse to each other.

+	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9	0
2	2	3	4	5	6	7	8	9	0	1
3	3	4	5	6	7	8	9	0	1	2
4	4	5	6	7	8	9	0	1	2	3
5	5	6	7	8	9	0	1	2	3	4
6	6	7	8	9	0	1	2	3	4	5
7	7	8	9	0	1	2	3	4	5	6
8	8	9	0	1	2	3	4	5	6	7
9	9	0	1	2	3	4	5	6	7	8

Addition table in Z_{10}

Similarly in multiplication table each cross sectional cell contains the multiplication operations followed by mod operation by n. From the table the multiplicative inverse will be the integers for which the result is 1.

×	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

Multiplication table in Z_7

In cryptography the sender can uses an integer as encryption key and the receiver uses the inverse of that integer as decryption key. Z_n can be used as a set of possible keys if the algorithm used in encryption or decryption is addition because each integer in this set has an additive inverse. But if the algorithm is multiplication then it is not possible to use $\mathbf{Z_n}$ as the set of possible keys because in Z_n all integers does not have multiplicative inverse. Here we can use another set consist of integers from Z_n which has multiplicative inverse, this set is called $\mathbf{Z_{n*}}$. For example,

$$\mathbf{Z_{10} = \{0,1,2,3,4,5,6,7,8,9\}} \qquad \mathbf{Z_{10*} = \{1,3,7,9\}}$$

- **Matrices :**

A matrix is the array of dimension $l \times m$, where l is the number of rows and m is the number of columns. A matrix is represented with a capital letter such as A. Each element of the matrices is denoted as $\boldsymbol{a_{ij}}$, it represents an element at i^{th} row and j^{th} column.

1. A matrices having only one row is called **row matrices**.

$$\begin{bmatrix} 64 & 45 & 32 & 12 \end{bmatrix}$$

2. A matrices having only one column is called **column matrices**.

$$\begin{bmatrix} 56 \\ 43 \\ 32 \\ 23 \end{bmatrix}$$

3. A matrices having same number of rows and column is called **Square matrices**.

$$\begin{bmatrix} 34 & 53 & 21 \\ 32 & 33 & 45 \\ 73 & 38 & 43 \end{bmatrix}$$

4. A matrices having all element set to 0's is called **additive identity matrices** denoted as **0**.

$$\begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}$$

5. Square matrices having 1's on the main diagonal elements and 0's elsewhere is called **identity matrices** denoted as ***I***.

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Operations and relations:

In linear algebra we can perform one relational and four mathematical operation on matrices,

Equality:

Two matrices are equal if they have same number of rows and column, and the corresponding elements are equal. I.e. two matrices A and B are said to be equal if the dimension of A and B are same and for every value of *i* and *j* we have $a_{ij} = b_{ij}$.

$$A=\begin{bmatrix} 2 & 5 \\ 3 & 8 \end{bmatrix} \qquad B=\begin{bmatrix} 2 & 5 \\ 3 & 8 \end{bmatrix}$$

Addition:

We can add two matrices *A* and *B* if the dimensions of two matrices are equal and the resulting matrices *C* will be of the same dimensions as *A* and *B*. Addition of two matrices are denoted as $\boldsymbol{C = A + B}$.
For every value of *i* and *j* the element of resulting matrices *C* is calculated from the element of *A* and *B* by the following formula,

$$\boldsymbol{c_{ij} = a_{ij} + b_{ij}}$$

$$A=\begin{bmatrix} 2 & 5 \\ 3 & 8 \end{bmatrix} \qquad B=\begin{bmatrix} 5 & 8 \\ 4 & 2 \end{bmatrix}$$

$$C=A+B=\begin{bmatrix} 2 & 5 \\ 3 & 8 \end{bmatrix} + \begin{bmatrix} 5 & 8 \\ 4 & 2 \end{bmatrix} = \begin{bmatrix} (2+5) & (5+8) \\ (3+4) & (8+2) \end{bmatrix} = \begin{bmatrix} 7 & 13 \\ 7 & 10 \end{bmatrix}$$

Subtraction:

As like the addition operation on two matrices *A* and *B* we can perform subtraction operation also denoted as $\boldsymbol{C=A-B}$.
In Subtraction operation for every value of *i* and *j* the element of resulting matrices C is calculated from the element of A and B by the following formula,

$$c_{ij}=a_{ij}-b_{ij}$$

$$A=\begin{bmatrix}2 & 5\\ 3 & 8\end{bmatrix} \qquad B=\begin{bmatrix}5 & 8\\ 4 & 2\end{bmatrix}$$

$$C=A-B=\begin{bmatrix}2 & 5\\ 3 & 8\end{bmatrix}-\begin{bmatrix}5 & 8\\ 4 & 2\end{bmatrix}=\begin{bmatrix}(2-5) & (5-8)\\ (3-4) & (8-2)\end{bmatrix}=\begin{bmatrix}-3 & -3\\ -1 & 6\end{bmatrix}$$

Multiplication:

The multiplication operation on two matrices is possible only if the number of column of the 1st matrices is same as the number of rows in the 2nd matrices. In other word if the dimension of the 1st matrices A is $l\times m$ then the dimension of the 2nd matrices B should be $m\times n$ and the dimension of the resultant matrices C will be $l\times n$.

$$c_{ik}=\sum a_{ij}\times b_{jk}$$

$$A=\begin{bmatrix}5 & 2 & 1\\ 3 & 2 & 4\end{bmatrix} \qquad B=\begin{bmatrix}7 & 3 & 2 & 1\\ 8 & 0 & 0 & 2\\ 1 & 3 & 4 & 0\end{bmatrix}$$

$$C=A\times B=\begin{bmatrix}5 & 2 & 1\\ 3 & 2 & 4\end{bmatrix}\times\begin{bmatrix}7 & 3 & 2 & 1\\ 8 & 0 & 0 & 2\\ 1 & 3 & 4 & 0\end{bmatrix}$$

$$=\begin{bmatrix}52 & 18 & 14 & 9\\ 41 & 21 & 22 & 7\end{bmatrix}$$

Scalar Multiplication:

With a matrix we can also multiply a scalar quantity (a number). If A is a matrix and x is a scalar then $C = x \times A$ is a resultant matrix in which $c_{ij} = x \times a_{ij}$

$$A=\begin{bmatrix}6 & 3 & 2\\ 3 & 7 & 9\end{bmatrix}$$

$$C=4\times A=4\times\begin{bmatrix}6 & 3 & 2\\ 3 & 7 & 9\end{bmatrix}=\begin{bmatrix}24 & 12 & 8\\ 12 & 28 & 36\end{bmatrix}$$

Determinant:

The determinant of a **square matrix A** of dimension $m\times n$ is a scalar quantity calculated by applying the following steps recursively.

- ***If m = 1 det(A) = a_1***
- ***If m>1 det(A) = $\sum_{i=1\ldots m}(-1)^{i+j}\times a_{ij}\times det(A_{ij})$***

$$\det\begin{bmatrix}5 & 2 & 1\\ 3 & 0 & -4\\ 2 & 1 & 6\end{bmatrix}$$

$$= (-1)^{1+1} \times 5 \times \det\begin{bmatrix}0 & -4\\ 1 & 6\end{bmatrix} + (-1)^{1+2} \times 2 \times \det\begin{bmatrix}3 & -4\\ 2 & 6\end{bmatrix} + (-1)^{1+3} \times 1 \times \det\begin{bmatrix}3 & 0\\ 2 & 1\end{bmatrix}$$

$$= (+1) \times 5 \times (+4) + (-1) \times 2 \times (+26) + (+1) \times 1 \times (+3)$$

$$= 20 - 52 + 3 = -29$$

Inverse:

Matrix has both Additive and multiplicative inverses

Additive Inverse:

Two matrices *A* and *B* are additive inverse if $\boldsymbol{A+B=0}$, in such case $\boldsymbol{b_{ij}=-a_{ij}}$ for all *i* and *j*. Additive inverse of $\boldsymbol{A}$ is denoted as $\boldsymbol{-A}$.

Multiplicative Inverse:

Two matrices A and B are multiplicative inverse if both are **square** matrices and multiplication operation on both matrices always yields an Identity Matrix. Multiplicative inverse of $\boldsymbol{A}$ is denoted as $\boldsymbol{A^{-1}}$.

$$\boldsymbol{A \times B = B \times A = I}$$

Residue Matrices:

Residue matrices are the matrices where all the elements of the matrices are from Z_n. The operations on residue matrices are same as integer matrices except that all the operations are performed as **modular arithmetic**.

A residue matrix has a multiplicative inverse if the determinant of the matrix has a multiplicative inverse in Z_n. That is if the $\boldsymbol{gcd(det(A), n) = 1}$ then the residue matrix has a multiplicative inverse.

Congruence Matrix:

Two matrices are said to be congruent modulo n denoted as $A \equiv B \ (mod\ n)$, if the matrices have same number of rows and columns and all the corresponding elements are congruent modulo *n*.

$$\boldsymbol{A \equiv B\ (mod\ n)\ \text{if}\ a_{ij} \equiv b_{ij}\ (mod\ n).}$$

- **Linear Congruence:**

In cryptography it is common to solving a equation or a set of equation of single or multiple variables with coefficient in Z_n

Single variable Linear equation:

It is the equation of the form $ax \equiv b \pmod n$. $GCD(a, n)=d$, if b is not divisible by d then there is no solution. And if $d \mid b$ we can find the solutions by the following steps,

1. Reduces the equation by dividing both sides by d.
2. Multiply both sides of the reduced equation by the multiplicative inverse of a to find the solution x_0.
3. The solutions are $x = x_0+k\ (n/d)$ for $k=0,1,\ldots,(d-1)$.

Set of Linear equation:

We can solve a set of linear equation by forming three matrices from the equations.

The first is the square matrix made from the coefficients of the variables.
The second matrix is a column matrix made from the variables.
The third matrix is a column matrix made from the value at the right-hand side of the equation.

We can implement the set of linear equation and can solve it by the matrix multiplication as follows,

Equations-

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &\equiv b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &\equiv b_2 \\ \cdot \quad\quad \cdot \quad\quad\quad\quad \cdot \quad\quad \cdot \\ \cdot \quad\quad \cdot \quad\quad\quad\quad \cdot \quad\quad \cdot \\ \cdot \quad\quad \cdot \quad\quad\quad\quad \cdot \quad\quad \cdot \\ a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nn}x_n &\equiv b_n \end{aligned}$$

Matrix Interpretation-

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} \equiv \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix}$$

Solution-

$$\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} \equiv \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}^{-1} \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix}$$

……Continued