Basic principles : Security Goals, Crytographic attacks, services and Mechanisms, Mathematics of cryptography.

Cryptography :

Cryptography is a method of protecting information and communications through the use of codes, so that only those for whom the information is intended can read and process it.

In computer science, Cryptography refers to secure information and communication techniques derived from mathematical concepts and a set of rule-based calculations called algorithms, to transform messages in ways that are hard to decipher. These deterministic algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on the internet and confidential communications such as credit card transactions and email.

Cryptography techniques

Cryptography is closely related to the disciplines of cryptology and Cryptanalysis. It includes techniques such as microdots, merging words with images and other ways to hide information in storage or transit. Cryptography is most often associated with plain text into Ciphertext (a process called encryption), then back again (known as decryption).

Modern cryptography concerns itself with the following four objectives:

1. Confidentiality:

The information cannot be understood by anyone for whom it was unintended

2. Integrity

The information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected

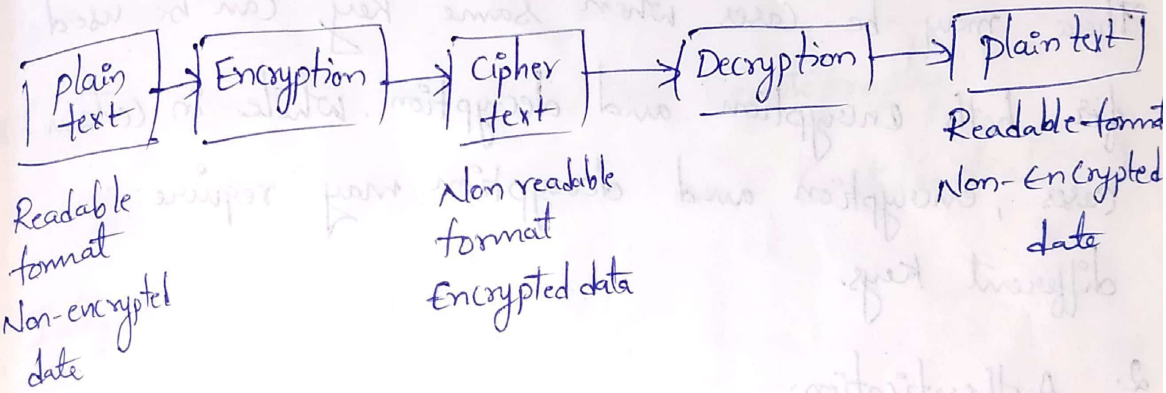
3. Non-repudiation:

The creator/sender of the information cannot deny at a later stage their intentions in the creation or transmission of the information

4. Authentication:

The sender and receiver can confirm each others identity and the origin/destination of the information

CRYPTOGRAPHY



Cryptography is the process of encrypting and decrypting data.

procedures and protocols that meet some or all of the above criteria are known as cryptosystems.

Basic principles:

1. Encryption

In a simplest form, encryption is to convert the data in some unreadable form. This helps in protecting the privacy while sending the data from sender to receiver. On the receiver side, the data can be decrypted and can be brought back to its original form. The reverse of encryption is called as decryption. The Concept of encryption and decryption requires some extra information for encrypting and decrypting the data. This information is known as key. There may be cases when same key can be used for both encryption and decryption while in certain cases, encryption and decryption may require different keys.

2. Authentication:

Authentication ensures that the message was originated from the originator claimed in the message. Suppose, Alice sends a message to Bob and now Bob wants proof that the message has been indeed sent by Alice. This can be made possible if Alice performs some action on message that Bob knows only Alice can do. Well, this forms the basic fundamental of Authentication.

3. Integrity

Communication system can face loss of integrity of messages being sent from sender to receiver. This means that cryptography should ensure that the messages that are received by the receiver are not altered anywhere on the communication path.

4. Non Repudiation:

what happens if Alice sends a message to Bob but denies that she has actually sent the message? Cases like these may happen and crypto-graphy should prevent the originator (or) sender to act this way.

*Security Goals (CIA triad in cryptography)

The three Security Goals are Confidentiality, Integrity and Availability

Confidentiality

It is the most common aspect of information security. It allows authorized users to access sensitive and protected data.

The data sent over the network should not be accessed by unauthorized users.

Attacker will try to capture data. To avoid this, various encryption techniques are used to safeguard our data. so that even if attacker gains access, he/she will not be able to decrypt it.

Integrity:

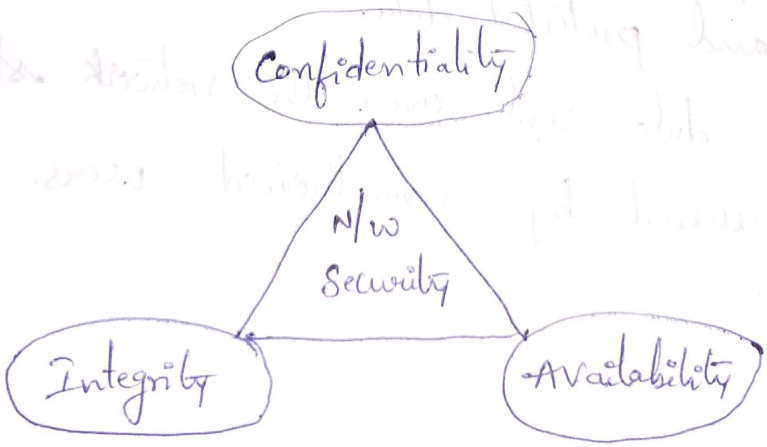
Integrity means that changes need to be done only by the authorized entities and through authorized Mechanisms and nobody else should modify our data

Eg: In a bank, when we deposit / withdraw Money, the balance needs to be maintained

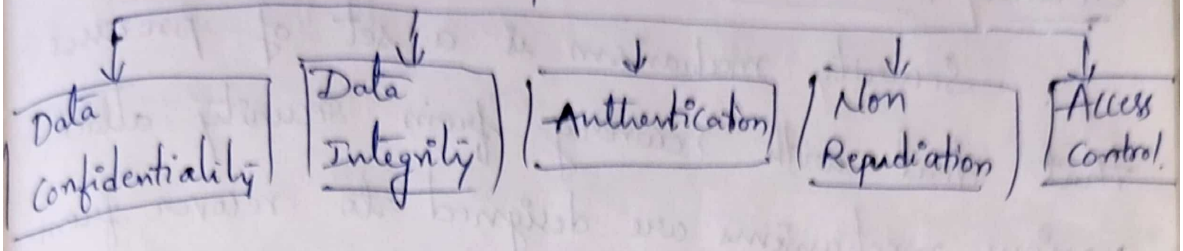
Availability

Data must be available to the authorized user. Information is useless if we cannot access it.

eg: what would happen if we cannot access our bank accounts for transactions



Security Services.



Authentication:

-Assures Recipient that the message is from the source that it claims to be from.

Access Control:

Controls who can have access to resource under what condition.

Availability

Data must be available to the authorized user

Confidentiality

Information should not made available to unauthorized user.

Integrity

Assurance that the message is unaltered

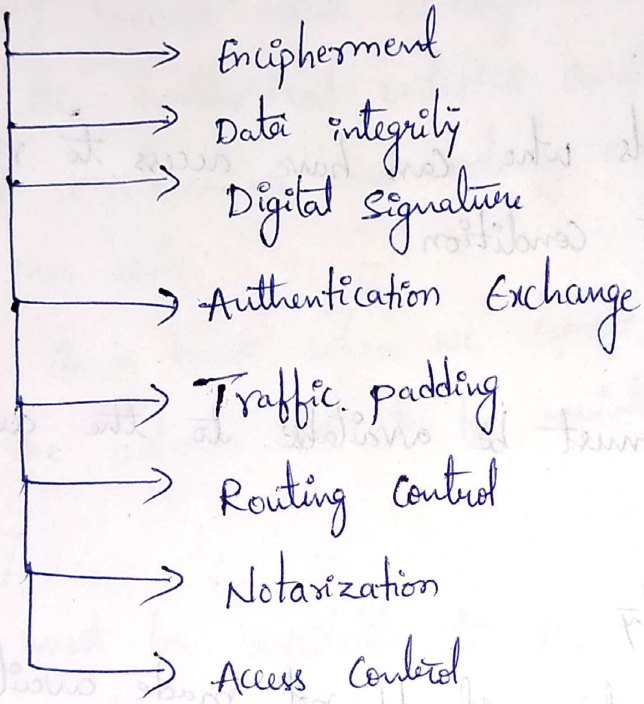
Non Repudiation

protetion against denial of sending or receiving information in the communication.

Security Mechanisms.

Security mechanism is a set of process that deal with recovery from security attack. Various mechanisms are designed to recover from these specific attacks at various protocol layers.

Security Mechanisms



Encipherment:

This security mechanism deals with hiding and covering of data which helps data to become confidential. It is achieved by applying mathematical calculations or algorithms which reconstruct information into not readable form. It is achieved by two famous techniques Cryptography and encipherment. Level of data

encryption is dependent on the algorithm used for encipherment.

Access Control

This mechanism is used to stop unattended access to data which you are sending. It can be achieved by various techniques such as applying passwords, using firewall, or just by adding PIN to data.

Notarization

This security mechanism involves use of trusted third party in communication. It acts as mediator between sender and receiver so that if any chance of conflict is reduced. This mediator keeps record of requests made by sender to receiver for later denied.

Data Integrity

This security mechanism is used by appending value to data to which is created by data itself. It is similar to sending packet of information known to both sending and receiving parties and checked before and after data is received. When this packet or data which is appended is checked and is the same while sending and receiving data integrity is maintained

Authentication Exchange

This security mechanism deals with identity to be known in communication. This is achieved at the TCP/IP layer where two-way handshaking mechanism is used to ensure data is sent or not.

Bit Stuffing

This security mechanism is used to add some extra bits into data which is being transmitted It helps data to be checked at the receiving end and is achieved by even parity or odd parity.

Digital signature

This security mechanism is achieved by adding digital data that is not visible to eyes It is form of electronic signature which is added by sender which is checked by receiver electronically. This mechanism is used to preserve data which is not more confidential but senders identity is to be notified.

Routing Control

It allows selection of specific physically secure routes for specific data transmission and enables routing changes, particularly when a gap of security is suspected.

Cryptographic attacks

A cryptographic attack allows the attacker to bypass the security of a cryptographic system by assessing the weakness in its cipher, cryptographic protocol, and key management scheme, a process also referred to as cryptanalysis

There are many different attacks that the attacker uses to bypass the security of a system Some of these attacks are as follows

- Known plain-text attack:

In this case, the attacker knows the plain text and cipher text and they try to calculate the key be reverse engineering the cipher.

- Cipher-Only attack:

The attacker known the cipher of different messages encrypted using the keys. They try to calculate the key using the ciphers provided.

- Chosen plain-text attack:

This attack is similar to the known plain-text attack, but now the attacker chooses a plain-text of their own choice and then generates the cipher against them using the key. Now the attacker tries to calculate the key using the Chosen plain text and the corresponding cipher

Chosen cipher-text attack:

The attacker chooses a cipher text and decrypted text portion of the cipher. The attacker then uses this to figure out the key.

Replay attack:

In this attack, the attacker captures some of the authentication information and resubmits it to the server to gain access to the information meant for the original owner only.

Brute force

It is the method of trying all the possible combinations to figure out the key. It may be relatively easier if the size of the key is smaller, but if the size of the key increases, it becomes computationally infeasible to test all the options.

Types of Cryptographic attacks

The cryptographic attacks can be classified into two categories based on their use case:

- Active attacks
- Passive attacks.

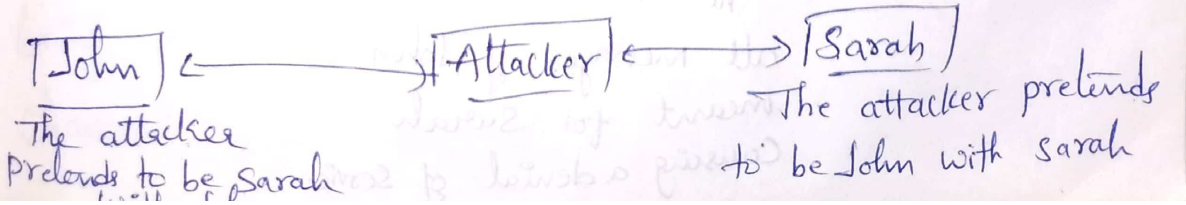
Active attacks

Active attacks occur when the attacker gets access to the communication channel between the two entities. The attacker acts as the man in the middle and can eavesdrop and tamper with the messages being sent on the channel between the entities. These attacks are relatively easy to detect but still are considered to be the more dangerous of the two, as the attacker can manipulate the data being shared and gain access or privileges.

Use cases of active attacks

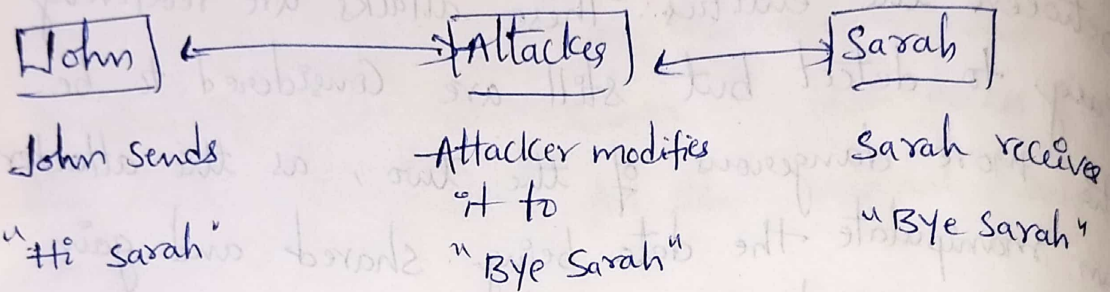
- **Masquerade:**

This attack occurs when the attacker pretends to be the sender, trying to convince the receiver that it is the sender. This is possible if the authorization procedure is not secure, as the attacker can pretend to be another entity using stolen passwords



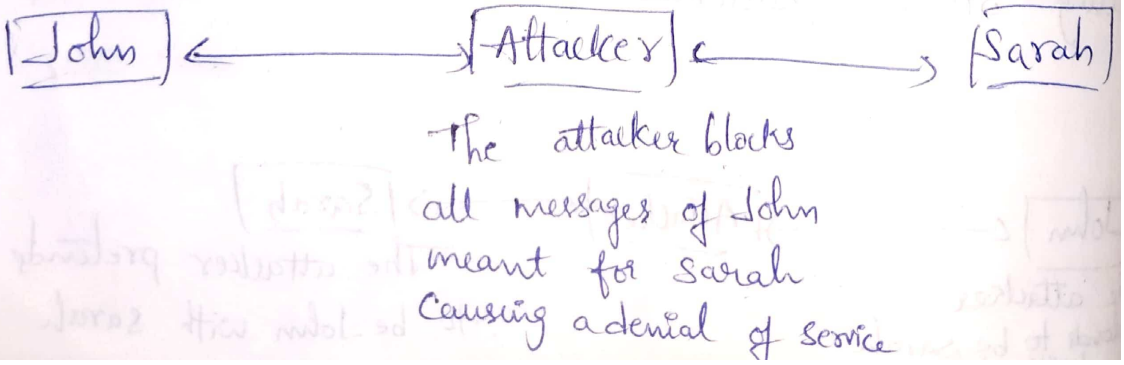
Modification of Messages:

Messages being shared between the two entities via a communication channel can be tampered with if the attacker gets access to the key used to encrypt / decrypt the messages



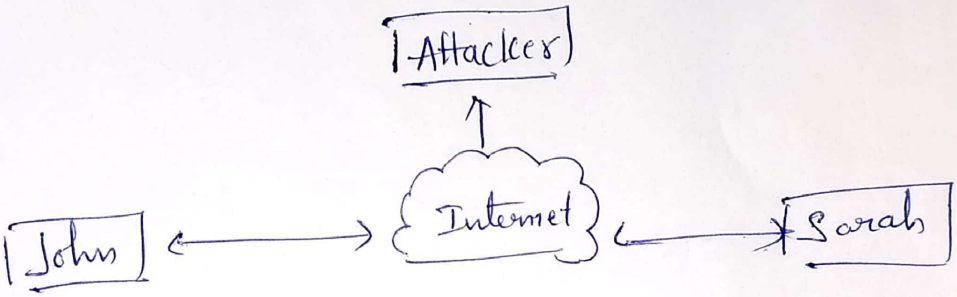
Denial-of-Service:

The attacker in the middle of both the entities can either completely stop the messages from one entity from reaching another or overload an entity by relaying a message multiple times to overload the receiving entity. Both these cases result in a denial of service



Passive Attack:

Passive Attacks occur when the user gets access to the communication channel between the two entities and can eavesdrop on the ongoing communication between the two entities. However, the attacker can't tamper with the messages in this case as was possible in the active attack. Passive attacks are harder to detect and cause little less damage than active attacks, but the confidentiality of the messages is lost.



Use cases of passive attacks:

- Traffic analysis

The attacker analyzes the traffic data, the origin and the destination IP address of the message. They also monitor and analyze the human and machine identities on both ends.

- Release of message Contents

The attacker listens to the information being shared on the compromised communication channel and releases the message's contents

- This means inserting some bogus data into the data traffic to the adversary's attempt to use the traffic analysis.

Routing control:

- It means selecting and continuously changing different available routes between sender and receiver to prevent the opponent from eavesdropping on a particular route.

Notarization:

- It means selecting a third trusted party to control the communication between two entities.
- This can be done, for example,to prevent repudiation.

Access control:

- It uses methods to prove that a user has access right to the data or resources owned by a system.
- Examples of proofs are passwords and PINs

➢ **Relation between Services and Mechanisms:**

Security Service	*Security Mechanism*
Data confidentiality	Encipherment and routing control
Data integrity	Encipherment, digital signature, data integrity
Authentication	Encipherment, digital signature, authentication exchanges
Nonrepudiation	Digital signature, data integrity, and notarization
Access control	Access control mechanism

❖ **<u>Mathematics of Cryptography:</u>**

Cryptography is based on some specific areas of mathematics, including number theory, linear algebra and algebraic structures.

Integer arithmetic: In integer arithmetic, we use a set and few operations.

Set of Integers: The set of integers, denoted by Z, contains all integral numbers(with no fraction)from negative infinity to positive infinity.

z={.....,-2,-1,0,1,2.....}

Binary operations: In cryptography , we are interested in three basic operations applied to the set of integers. A binary operation takes two inputs and creates one output.

- Three basic operations are addition, subtraction and multiplication. Each of these operations takes 2 inputs and creates 1 output.
- The two inputs come from the set of integers; the output goes into the set of integers.

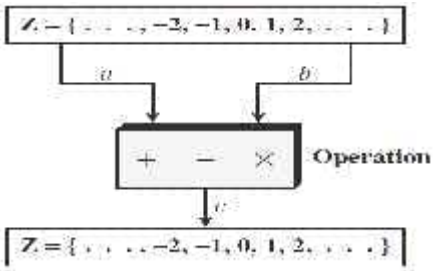


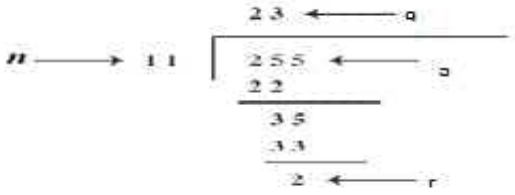
fig: Three binary operations for the set of integers

- **Integer Division**:

  In integer arithmetic, if we divide a by n, we get q and r. The relationship between these four integers can be shown as

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

  In this relation , a is called the dividend; q, the quotient; the divisor; and r, the remainder.



  Two Restrictions: For our purpose,we impose two restrictions.First,we require that the divisor be a positive integer($n>0$). Second,we require that the remainder be a non-negative integer($r \geq 0$).

- **Divisibility:** If a is not zero and we let r=0 in the division relation, we get

$$a=q\times n$$

  we say that n divides a.we can also say that a is divisible by n.when we are not interested in the value of q,we can write the above relationship as a|n.If the remainder is not zero,then n does not divide a and we can write the relationship as a×n.

Properties:

- If a|1, then a = ±1.
- If a|b and b|a, then a = ±b.
- If a | b and b | c, then a | c
- If a|b and a|c, then a|(m×b + n×c) where m and n are arbitrary integers.

Example:

a. Since 3|15 and 15|45,according to third property, 3|45

b. Since 3|15 and 3|9 , according to fourth property, 3|(15×2+9×4),which means 3|66

- **Greatest Common Divisor:** One integer often needed in cryptography is the greatest common divisor of two positive integers. Two positive integers may have many common divisors, but only one greatest common divisor.

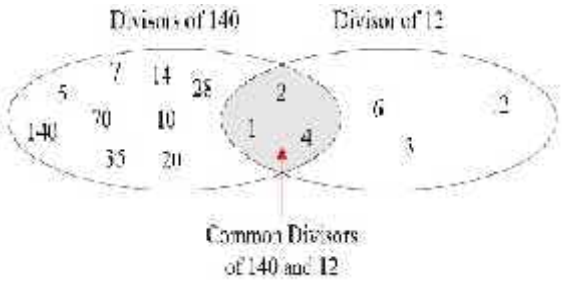


fig:Common divisors of two integers

Note: The greatest common divisor of two positive integers is the largest integer that can divide both integers

- **Euclidean Algorithm:** Finding the greatest common divisor (gcd) of two positive integers by listing all common divisors is not practical when two integers are large.

Fact 1: gcd(a,0)=a Fact 2: gcd(a,b)=gcd(b,r),where r is the remainder of dividing a by b

The first fact tells us that if the second integer is 0, the greatest common divisor is the first one.The second fact allows us to change the value of a,b until b becomes 0.

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

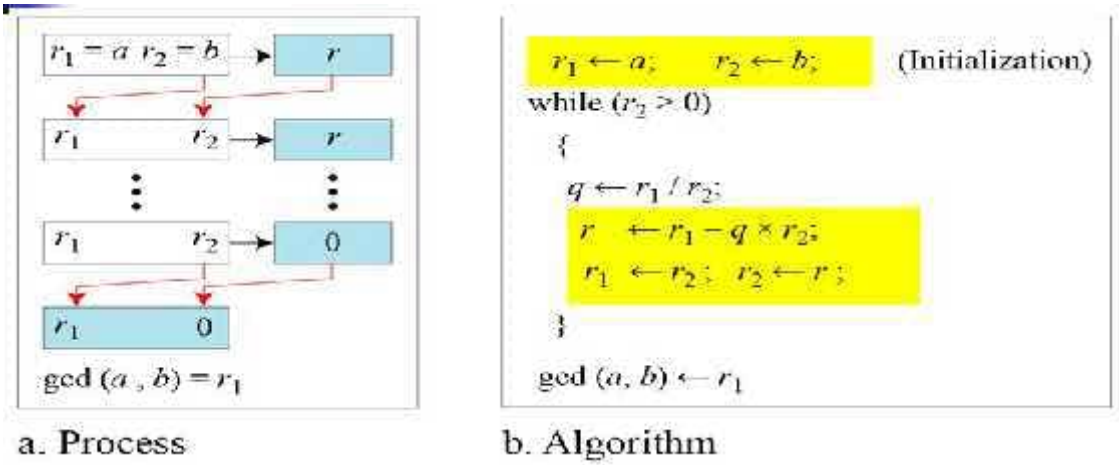


fig: 2.7 Euclidean algorithm

- we use two variables r1 and r2, to hold the changing values during the process of reduction.They are initialized to a and b.
- In each step, we calculate the remainder of r1 divided by r2 and store the result in the variable r.we then replace r1 by r2 and r2 by r.

- The steps are continued until r2 becomes 0.At this moment,we stop. The gcd(a,b) is r1.

  when gcd(a,b) = 1, we say that a and b are relatively prime

  Example : Find the greatest common divisor of 2740,1760

  sol:

We have gcd (2740, 1760) = 20

q	r_1	r_2	r
1	2740	1760	980
1	1760	980	780
1	980	780	200
3	780	200	180
1	200	180	20
9	180	20	0
	20	0	

- **The Extended Euclidean Algorithm:**

Given two integers a and b,we often need to find other two integers, s and t, such that

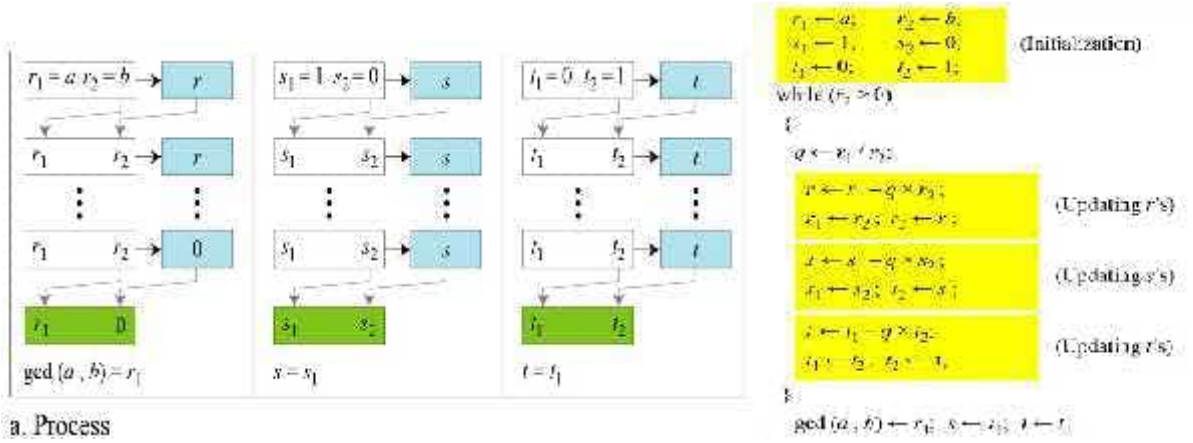
$$s \times a + t \times b = \gcd(a,b)$$

The Extended euclidean algorithm can calculate the gcd(a,b) and at the same time calculate the value of s and t. The algorithm and the process is shown below diagram.

- The extended euclidean algorithm uses the same number of steps as the Euclidean algorithm. However in each step , we use three sets of calculations and exchange instead of one.
- The algorithm uses three sets of variables, r's, s's and t's.
- In each step r_1,r_2 and r have the same values in the Euclidean algorithm.
- The variables r_1 and r_2 are initialized to the values of a and b respectively.
- The variables s_1 and s_2 are initialized to 1 and 0 respectively.

- The variables t_1 and t_2 are initialized to 1 and 0 respectively.
- The calculations of r, s and t are similar, with one warning.

Although r is the remainder of dividing r_1 and r_2, there is no such relationship between the other two sets. There is only one quotient, q, which is calculated $r_1|r_2$ and used for the other two calculations.



Given $a = 161$ and $b = 28$, find gcd (a, b) and the values of s and t.

Solution

We get gcd $(161, 28) = 7$, $s = -1$ and $t = 6$.

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
5	161	28	21	1	0	1	0	1	−5
1	28	21	7	0	1	−1	1	5	6
3	21	7	0	1	−1	4	−5	6	−23
	7	0		−1	4		6	−23	

$r=r_1-q\times r_2$ $s=s_1-q\times s_2$ $t=t_1-q\times t_2$

- **Linear Diophantine Equations:**

Although we will see a very important application of the extended Euclidean algorithm. One immediate applications is to find the solutions to the linear Diophantine equations of two variables, an equation of type ax+by+c.we need to find integer values for x and y that satisfy the equation.This type of equation has either no solution or an infinite number of solutions.

Let d= gcd(a,b) , If d+c, then the equation has no solution.

If d|c , then we have an infinite number of solutions. one of them is called the particular; the rest, general

A linear Diophantine equation of two variables is ax+by=c.

- **MODULAR ARITHMETIC:**

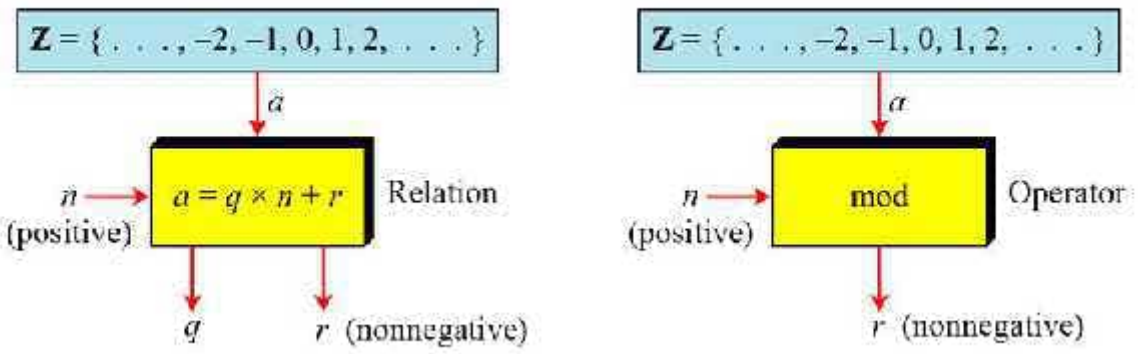
- The division relationship (a=q × n+r) has two inputs (a and n) and two outputs (q and r).
- In modular arithmetic , we are intereted in only one of the outputs, the remainder r.we don't care about the quotient q.
- In other words , we want to know what is the value of r when we divide a by n.
- This implies that we can change the above relation into a binary operator with two inputs a and n and one output r.

Modulo Operator:

- The above mentioned binary operator is called the **modulo operator** and is shown as **mod.**
- The second input (n) is called the modulus. The output r is called the residue.
- The below figure shows , the modulo operator (mod) takes an integer (a) from the set z and a positive modulus (n) .The operator creates a nonnegative residue (r) .we can say

a mod n = r

Figure 2.9 *Division algorithm and modulo operator*



Set of Residues: $\mathbf{Z_n}$

- The result of the modulo operation with modulus n is always an integer between 0 and n-1.
- In other words, the result of a mod n is always a nonnegative integer less than n.
- we can say that the modulo operation creates a set, which in modular arithmetic is referred to as the set of least residues modulo n, or Z_n.
- We have infinite instances of the set of residues (Z_n),one for each value of n.
- The below figure shows the set Z_n and three instances, Z_2,Z_6, and Z_{11}.

Figure 2.10 *Some Z_n sets*

$Z_n = \{0, 1, 2, 3, \ldots, (n-1)\}$

$Z_2 = \{0, 1\}$ $Z_6 = \{0, 1, 2, 3, 4, 5\}$ $Z_{11} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

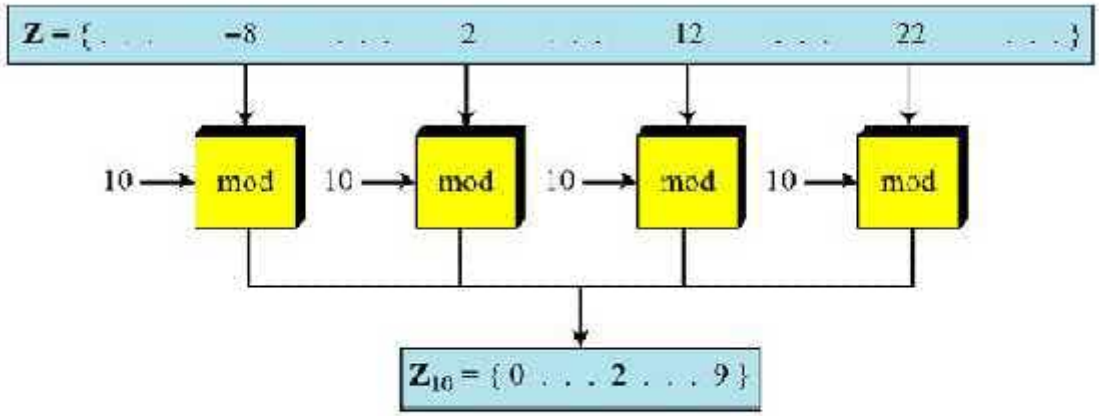
Congruence:

- In Cryptography, we often used the concept of congruence instead of equality.
- Mapping from Z to Z_n is not one-to-one.
- For example, the result of 2 mod 10 = 2,12 mod 10 = 2,22 mod 2= 2,and so on.
- In Modular arithmetic , integers like 2,12, and 22 are called congruent mod 10.
- To show that two integers congruent, we use the congruence operator (≡).
- We add the phrase (mod n) to the right side of the congruence to define the value of modulus that makes the relationship valid. For example ,we write:

$2 \equiv 12 \pmod{10}$	$13 \equiv 23 \pmod{10}$	$34 \equiv 24 \pmod{10}$	$-8 \equiv 12 \pmod{10}$
$3 \equiv 8 \pmod{5}$	$8 \equiv 13 \pmod{5}$	$23 \equiv 33 \pmod{5}$	$-8 \equiv 2 \pmod{5}$

we need to explain several points.

- The congruence operator looks like the equality operator, but there are differences. First, an equality operator maps a member of Z to itself; the congruence operator maps a member from Z to member of Zn. Second, the equality operator is one-to-one ; the congruence operator is many-to-one.
- The phrase (mod n) that we insert at the right-hand-side of the congruence operator is just an indication of the destination set (Zn).



Residue classes:

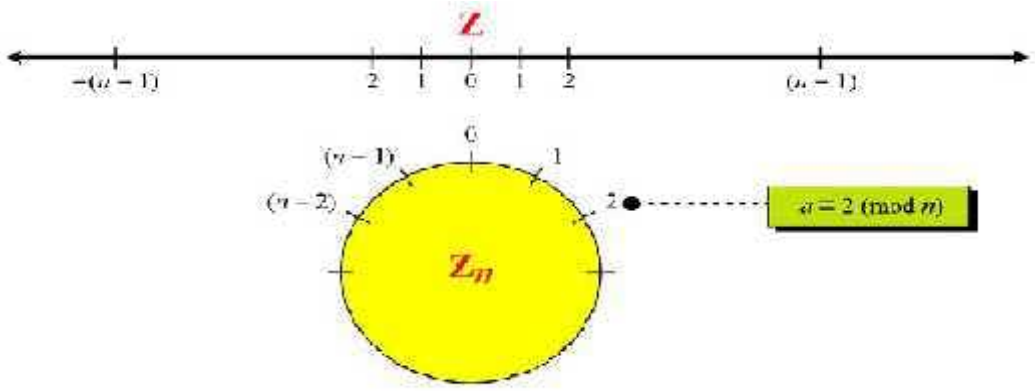
- A residue calss [a] or $[a]_n$ is the set of integers congruent modulo n. In other words, it is the set of all integers such that x = a (mod n). For example, if n=5, we have five sets [0],[1],[2],[3], and [4] as shown below:

$$[0] = \{\ldots, -15, -10, -5, 0, 5, 10, 15, \ldots\}$$
$$[1] = \{\ldots, -14, -9, -4, 1, 6, 11, 16, \ldots\}$$
$$[2] = \{\ldots, -13, -8, -3, 2, 7, 12, 17, \ldots\}$$
$$[3] = \{\ldots, -12, -7, -5, 3, 8, 13, 18, \ldots\}$$
$$[4] = \{\ldots, -11, -6, -1, 4, 9, 14, 19, \ldots\}$$

- The integers in the set [0] are all reduced to 0 when we apply the modulo 5 operation on them. The integers in the set [1] are all reduced to a when we apply the modulo 5 operation, and so on.
- In each set, there is one element called the least(non negative) residue.
- In the set [0], this element is 0; in the set [1], this element is 1; and so on.
- The set of all of these least residues is what we have shown as $Z_5 = \{0,1,2,3,4\}$.
- In other words , the set Z_n is the set of all least residue modulo n.

Circular Notation:

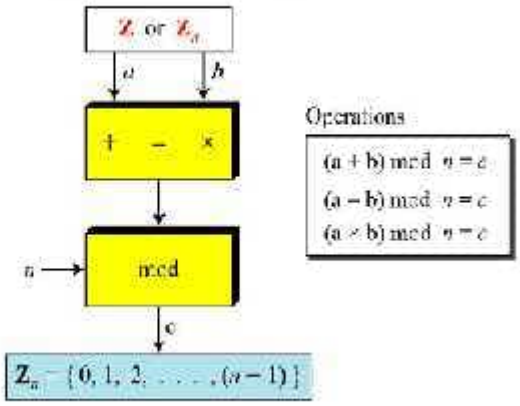
- The concept of congruence can be better understood with the use of a circle.
- we can use a circle to show the distribution of integers in Z_n.
- The below figure shows the comparison between the two. Integers 0 to n-1are spaced evenly around a circle.
- All congruent integers modulo n occupy the same point on the circle.
- Positive and negative integers from Z are mapped to the circle in such a way that there is a symmetry between them.



Operations in Z_n:

- The three binary operations(addition, subtraction and multiplication) that we discussed for the set Z can also be defined for the set Z_n.
- The result may need to be mapped to Z_n using the mod operator as shown

Figure 2.13 *Binary operations in Z_n*



- Actually the two sets of operators are used here.
- The first set is one of the binary operators (+,-,×); the second is the mod operator.
- we need to use paranthesis to emphasize the order of operations.

Perform the following operations (the inputs come from Zn):
a. Add 7 to 14 in Z15.
b. Subtract 11 from 7 in Z13.
c. Multiply 11 by 7 in Z20.

Solution The following shows the two steps involved in each case

$$(14 + 7) \bmod 15 \rightarrow (21) \bmod 15 = 6$$
$$(7 - 11) \bmod 13 \rightarrow (-4) \bmod 13 = 9$$
$$(7 \times 11) \bmod 20 \rightarrow (77) \bmod 20 = 17$$

Properties:

- we mentioned that the two inputs to three binary operations in the modular arithmetic can come from Z or Z_n.
- The following properties allow us to first map the two inputs to Z_n before applying the three basic operations (+,-,×).

$$\text{First Property: } (a + b) \bmod n = [(a \bmod n) + (b \bmod n)] \bmod n$$
$$\text{Second Property: } (a - b) \bmod n = [(a \bmod n) - (b \bmod n)] \bmod n$$
$$\text{Third Property: } (a \times b) \bmod n = [(a \bmod n) \times (b \bmod n)] \bmod n$$

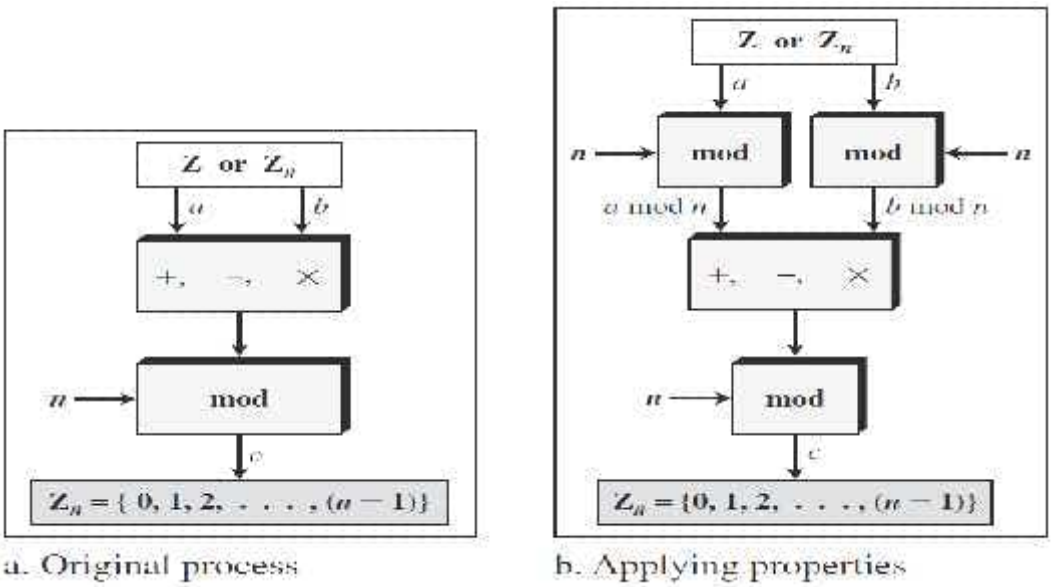


fig: Properties of mod operator

- The above figure shows the process before and after applying the above properties.
- Although the figure shows that the process is longer if we apply the above properties,we should remember that in cryptography we are dealing with very large integers.
- For example,if we multiply a very large integer by another very large integer , we have an integer that is too large to be stored in computer.
- The properties allow us to work with small numbers.

The following shows the application of the above properties:

1. (1,723,345 + 2,124,945) mod 11 = (8 + 9) mod 11 = 6
2. (1,723,345 − 2,124,945) mod 11 = (8 − 9) mod 11 = 10
3. (1,723,345 × 2,124,945) mod 11 = (8 × 9) mod 11 = 6

Inverses:

- when we are working in modular arithmetic, we often need to find the inverse of a number relative to an operation.
- we are normally looking for an **additive inverse** or a **multiplicative inverse.**

Additive inverse:

- In Z_n, two numbers a and b are additive inverses of each other if $a+b \equiv 0 \pmod{n}$
- In Z_n, the additive inverse of a can be calculated as b=n-a. For example , the additive inverse of 4 in Z_{10} is 10-4=6.

In modular arithmetic, each integer has an additive inverse. The sum of an integer and its additive inverse is congruent to 0 modulo n.

Note that in modular arithmetic, each number has an additive inverse and the inverse is unique; each number has one and only one additive inverse. However the inverse of the number may be the number itself.

Example 2.21 Find all additive inverse pairs in Z_{10}.

Solution The six pairs of additive inverses are (0, 0), (1, 9), (2, 8), (3, 7), (4, 6), and (5, 5). In this list, 0 is the additive inverse of itself; so is 5. Note that the additive inverses are reciprocal; if 4 is the additive inverse of 6, then 6 is also the additive inverse of 4.

Multiplicative Inverse:

- In Z_n, two numbers a and b are multiplicative inverses of each other if
$$a \times b \equiv 1 \pmod{n}$$
- For example, if the modulus is 10,then the multiplicative inverse of 3 is 7.In other words,we have $(3 \times 7) \bmod 10 = 1$.

In modular arithmetic, an integer may or may not have a multiplicative inverse. when it does, the product of the integer and its multiplicative inverse is congruent to 1 modulo n.

It Can be proved that a has a multiplicative inverse in Z_n if and only if gc(n,a)=1.In this case, a and n are said to be **relatively prime**.

Example 2.22

Find the multiplicative inverse of 8 in Z_{10}.

Solution

There is no multiplicative inverse because gcd (10, 8) = 2 ≠ 1. In other words, we cannot find any number between 0 and 9 such that when multiplied by 8, the result is congruent to 1.

Example 2.23

Find all multiplicative inverses in Z_{10}.

Solution

There are only three pairs: (1, 1), (3, 7) and (9, 9). The numbers 0, 2, 4, 5, 6, and 8 do not have a multiplicative inverse.

The integer a in Z_n has a multiplicative inverse if and only if gcd(n,a) ≡ 1(mod n)

The extended Euclidean algorithm we can find the multiplicative inverse of b in Zn when n and b are given and inverse exists. when n and b are given and the inverse exists.

To show this, let us replace the first integer a with n(the modulus). we can say that the algorithm can find s and t such $s \times n + b \times t = \gcd(n,b)$.

However, if the multiplicative inverse of b exists, gcd(n,b) must be 1. so the relationship is

$(s \times n) + (b \times t) = 1$

Now we apply the modulo operator to both sides. In other words, we map each side to Z_n. We will have

$(s \times n + b \times t) \bmod n = 1 \bmod n$

$[(s \times n) \bmod n] + [(b \times t) \bmod n] = 1 \bmod n$

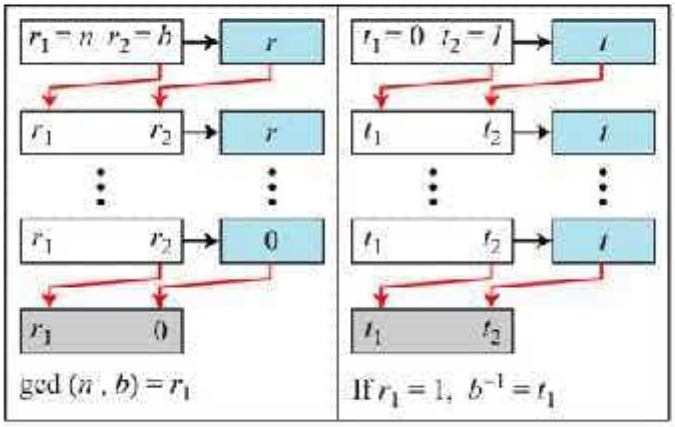
$0 + [(b \times t) \bmod n] = 1$

$(b \times t) \bmod n = 1$ → This means t is the multiplicative inverse of b in Z_n

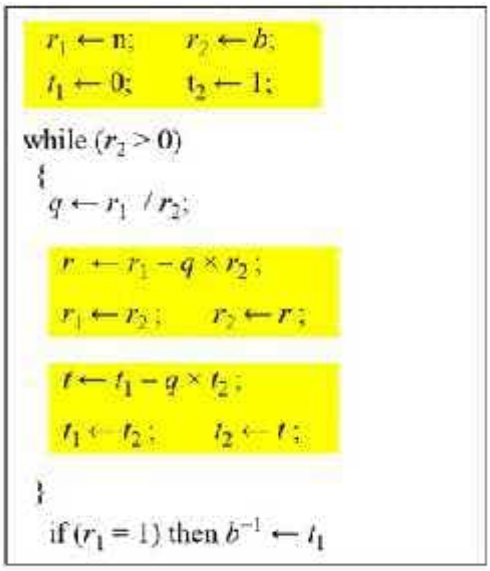
Note that $[(s \times n) \bmod n]$ in the third line is 0 because if we divide $(s \times n)$ by n, the quotient is s but the remainder is 0.

The extended Euclidean algorithm finds the multiplicative inverses of b in Z_n when n and b are given and gcd(n,b)= 1.The multiplicative inverse of b is the value of t after being mapped to Z_n.

fig: using the extended Euclidean algorithm to find the multiplicative inverse



a. Process



b. Algorithm

Example:

Find the multiplicative inverse of 11 in Z_{26}.

Solution

q	r_1	r_2	r	t_1	t_2	t
2	26	11	4	0	1	−2
2	11	4	3	1	−2	5
1	4	3	1	−2	5	−7
3	3	1	0	5	−7	26
	1	0		−7	26	

The gcd(26,11) is 1, which means that the multiplicative inverse of 11 exists. The extended Euclidean algorithm gives t_1 = -7. The multiplicative inverse is (-7)mod 26=19.In other words, 11 and 19 are multiplicative inverse in Z_{26}.we can see that (11 × 19)mod 26=209 mod 26=1.

Addition And Multiplication Tables:

- In addition table, each integer has an additive inverse. The inverse pairs can be found when the result of addition is zero.
- In multiplication table, we have only three multiplicative pairs(1,1),(3,7),(9,9).The pairs can be found whenever the result of multiplication is 1.
- Both tables are symmetric with respect to the diagonal of elements that moves from the top left to bottom right, revealing the commutative property for addition and multiplication (a+b=b+a and a × b =b × a).
- The addition table also shows that each row or column is a permutation of another row or column.This is not true for the multiplication table.

Addition and multiplication tables for Z_{10}

+	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 $\mathbf{Z_{10}}$

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

Multiplication Table in $\mathbf{Z_{10}}$

Different Sets For Addition And Multipliation:

- In cryptography, we often work with inverses.
- If the sender uses an integer, the receiver uses the inverse of that integer .
- If the operation is addition, Z_n can be used as the set of possible keys because each integer in this set has an additive inverse.
- If the operation is multiplication, Z_n cannot be the set of possible keys because only some members of this set have a multiplicative inverse.

We need to use Z_n when additive inverses are needed; we need to use Z_n^* when multiplicative inverses are needed.

fig: some Z_n and Z_n^* sets

$\mathbf{Z_6} = \{0, 1, 2, 3, 4, 5\}$

$\mathbf{Z_6^*} = \{1, 5\}$

$\mathbf{Z_7} = \{0, 1, 2, 3, 4, 5, 6\}$

$\mathbf{Z_7^*} = \{1, 2, 3, 4, 5, 6\}$

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

$\mathbf{Z_{10}^*} = \{1, 3, 7, 9\}$

Two more sets:

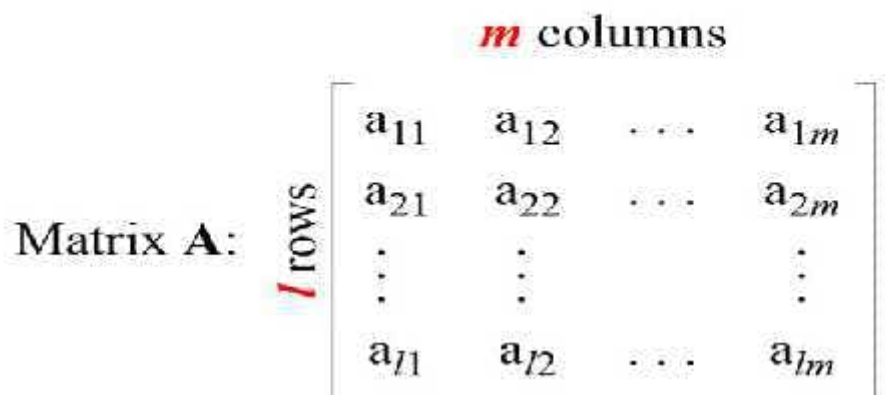
- The set Z_p is same as Z_n except that n is prime. Z_p contains all integers from 0 to p-1.Each member in Z_p has an additive inverse; each member except 0 has a multiplicative inverse.
- The set Z_p^* is same as Z_n^* except that n is prime. Z_p^* contains all integers from 1 to p-1.Each member in Z_p^* has an additive and multicative inverse.
- The following shows these two sets when p=13
  $Z_{13} = \{0,1,2,3,4,5,6,7,8,9,10,11,12\}$
  $Z_{13}^* = \{1,2,3,4,5,6,7,8,9,10,11,12\}$

➢ **MATRICES:**

Def: A matrix is a rectangular array of $l \times m$ elements, in which l is the number of rows and m is the number of columns.

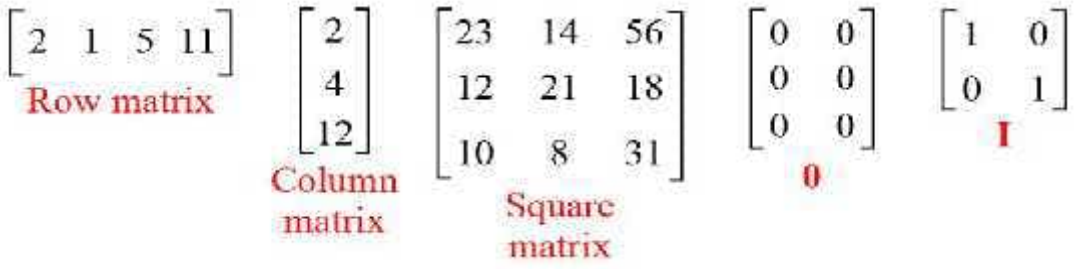
A matrix is normally denoted with a boldface uppercase letter such as **A.** The element a_{ij} is located in the ith row and jth column.Although the elements can be a set of numbers.

Figure 2.18 *A matrix of size l x m*



- If a matrix has only one row(l=1),it is called a row matrix; if it has only one column (m=1) it is called column matrix.
- In a square matrix, in which there is the same number of rows and columns (l=m)
- An additive identity matrix, denoted as 0,is a matrix with all rows and columns set to 0's.
- An identity matrix, denoted as I, is a square matrix with 1sbon the main diagonal and 0s elsewhere.

Figure 2.19 *Examples of matrices*



Operations and Relations:

In linear algebra,one relation and four operations(addition,subtraction,multiplication and scalar multiplication) are defined for matrices.

- **Equality:** Two matrices are equal if they have the same number of rows and columns and the corresponding elements are equal. In other words, A=B if we have $a_{ij}=b_{ij}$ for all i'a and j's.
- **Addition and Subtraction:** Two matrices can be added if they have the same number of columns and rows. This addition is shown as C=A+B.
- In this case,the resulting matrix C has also the same number of rows and columns as A or B.
- Each element of C is the sum of two correponding elements of A and B: $C_{ij} = a_{ij} + b_{ij}$.
- Subtraction is the same except that each element of B is subtracted from the corresponding element of A:dij = a_{ij} - b_{ij}

Example 2.28

Figure 2.20 shows an example of addition and subtraction.

Figure 2.20 *Addition and subtraction of matrices*

$$\begin{bmatrix} 12 & 4 & 4 \\ 11 & 12 & 30 \end{bmatrix} = \begin{bmatrix} 5 & 2 & 1 \\ 3 & 2 & 10 \end{bmatrix} + \begin{bmatrix} 7 & 2 & 3 \\ 8 & 10 & 20 \end{bmatrix}$$

C = A + B

- **Multiplication:**
  we can multiply two matrices of different sizes if the number of columns of the first matrix is the same as the number of rows of the second matrix.
  if A is an l × m matrix and B is m × p matrix, the product of the two is a matrix C of size l × p.
  If each element of matrix A is called aij ,each element of matrix B is called bjk,then each element of matrix C , Cij, can be calculated as
  cik = ∑ aij × bij =ai1 × b ij + ai2 × b 2j +.....+ aim × b mj

Example:

shows the product of a row matrix (1 × 3) by a column matrix (3 × 1). The result is a matrix of size 1 × 1.

Figure 2.21 *Multiplication of a row matrix by a column matrix*

$$\underset{C}{\begin{bmatrix}53\end{bmatrix}} = \underset{A}{\begin{bmatrix}5 & 2 & 1\end{bmatrix}} \times \underset{B}{\begin{bmatrix}7\\8\\2\end{bmatrix}}$$

- Scalar Multiplication:

We can also multiply a matrix by a number(called a scalar).If A is an l × m matrix and x is scalar, C=xA is a matrix of size l × m,in which cij= x * aij.

$$\underset{B}{\begin{bmatrix}15 & 6 & 3\\9 & 6 & 12\end{bmatrix}} = 3 \times \underset{A}{\begin{bmatrix}5 & 2 & 1\\3 & 2 & 4\end{bmatrix}}$$

Determinant: The determinant of a square matrix A of size m x m denoted as det(A) is scalar calculated recursively as shown below:

1. If m=1 , $\det(A)=a_{11}$
2. If m>1, $\det(A) = \sum(-1)^{i+j} \times a_{ij} \times \det(A_{ij})$

where A_{ij} is a matrix obtained from A by deleting the i^{th} row and j^{th} column.

example: we can calcualte the deteminant of a 2X 2 matrix

$$\det\begin{bmatrix}5 & 2\\3 & 4\end{bmatrix} = (-1)^{1+1} \times 5 \times \det[4] + (-1)^{1+2} \times 2 \times \det[3] \longrightarrow 5 \times 4 - 2 \times 3 = 14$$

or $$\det\begin{bmatrix}a_{11} & a_{12}\\a_{21} & a_{22}\end{bmatrix} = a_{11} \times a_{22} - a_{12} \times a_{21}$$

Inver

Inverses:

Matrices have both additive and multiplicative inverses.

Additive inverse:

The additive inverse of matrix A is another matrix B such that A+ B = 0.In other words, we have $b_{ij} = -a_{ij}$ for all values of i and j. Normally the additive inverse of A is defined by -A.

Multiplicative inverse:

The multiplicative inverse is defined only for square matrices. The multiplicative inverse of a square matrix A is a square matrix B such that AxB=BxA=I.

Normally the multiplicative inverse of A is defined by A^{-1}.However , matrices with real elements have inverses only if det(A) ≠ 0.

Multiplicative inverses are only definded for square matrix

Residue Matrices:

Cryptography uses residue matrices: matrices with all elements are in Z_n . All operations on residue matrices are performed the same as for the integer matrices except that the operations are done in modular arithmetic. The residue matrix has a multiplicative inverse if gcd(det(A),n)=1.

Example

A residue matrix and its multiplicative inverse in Z_{26}

$$\mathbf{A} = \begin{bmatrix} 3 & 5 & 7 & 2 \\ 1 & 4 & 7 & 2 \\ 6 & 3 & 9 & 17 \\ 13 & 5 & 4 & 16 \end{bmatrix} \qquad \mathbf{A}^{-1} = \begin{bmatrix} 15 & 21 & 0 & 15 \\ 23 & 9 & 0 & 22 \\ 15 & 16 & 18 & 3 \\ 24 & 7 & 15 & 3 \end{bmatrix}$$

$$\det(\mathbf{A}) = 21 \qquad \det(\mathbf{A}^{-1}) = 5$$

Congruence: Two matrices are congruent modulo n, written as A≡ B(mod n) , if they jave the same number of rows and columns and all corresponding elements are congruent modulo n. In other words A≡ B(mod n) if $a_{ij} \equiv b_{ij}$ for all i's and j's.

- **Linear Congruence:**

  Single Variable Linear Equations:

Let us see how we can solve equations involving a single variable—that is, equations of the form $ax \equiv b \pmod{n}$. An equation of this type might have no solution or a limited number of solutions. Assume that the gcd $(a, n) = d$. If d + b, there is no solution. If $d \mid b$, there are d solutions.

If $d \mid b$, we use the following strategy to find the solutions:

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

Example 2.35 Solve the equation $10x \equiv 2 \pmod{15}$.

Solution First we find the gcd (10 and 15) = 5. Since 5 does not divide 2, we have no solution.

Example 2.36 Solve the equation $14x \equiv 12 \pmod{18}$.

Solution Note that gcd (14 and 18) = 2. Since 2 divides 12, we have exactly two solutions, but first we reduce the equation.

$$14x \equiv 12 \pmod{18} \rightarrow 7x \equiv 6 \pmod{9} \rightarrow x \equiv 6\,(7^{-1}) \pmod{9}$$
$$x_0 = (6 \times 7^{-1}) \bmod 9 = (6 \times 4) \pmod{9} = 6$$
$$x_1 = x_0 + 1 \times (18/2) = 15$$

Both solutions, 6 and 15 satisfy the congruence relation, because $(14 \times 6) \bmod 18 = 12$ and also $(14 \times 15) \bmod 18 = 12$.

Set of linear equations:

- we can also solve a set of linear equations with the same modulus if the matrix formed from the coefficients of the variables is invertible.
- we make three matrices. The first is the square matrix made from the coeffients of varibles
- The second is a column matrix made from the variables.
- The third is a column matrix made from the values at the right - hand side of the congruence operator.
- We can interpret the set of equations as matrix multiplication.
- If both sides of congruence are multiplied by the multiplicative inverse of the first matrix, the result is the variable matrix at the right hand side, which means the problem can be solved by a matrix multiplication as shown below

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

a. Equations

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

b. Interpretation c. Solution

Fig. 2.27 *Set of linear equations*

Example 2.38 Solve the set of following three equations:

$3x + 5y + 7z \equiv 3 \pmod{16}$
$x + 4y + 13z \equiv 5 \pmod{16}$
$2x + 7y + 3z \equiv 4 \pmod{16}$

Solution Here x, y, and z play the roles of x_1, x_2, and x_3. The matrix formed by the set of equations is invertible. We find the multiplicative inverse of the matrix and multiply it by the column matrix formed from 3, 5, and 4. The result is $x \equiv 15 \pmod{16}$, $y \equiv 4 \pmod{16}$, and $z \equiv 14 \pmod{16}$. We can check the answer by inserting these values into the equations.