Introduction :-

Computer security vs Network security.

→ Computer security : generic name for collection of tools designed to protect data.

→ Network security : measures to protect data during transmission

→ Internet security : transmission over a collected of interconnected networks.

→ OSI Security Architecture :

Aspects of security :

1. security attack — active / passive
2. security mechanisms
3. security services.

Security Attack :

- any action that compromises the security of info owned by an organization.

passive : attacker will only steal/copy your data only will not modify or pretend as you to send manipulated data to the receiver.

active : can copy | steal | modify data. Resend modified data under your identity to the receiver.

attacker Replays the message as the intended sender → Data Integrity prob - active attack

passive attack — confidentiality problem.

→ Security service :

- enhance security of data processing systems & information transfers of an organisation

security mechanism - ensures { data authentication ⇒ verifying genuine user
" confidentiality → No other attacker should be able to know & read data while transmission
" integrity.

Security services

1. X.800 : offered by protocol layer - data transmission

2. RFC 2828 : sitting on the system provides security services to the system

Security Mechanisms (X.800)

- specific security mechanisms.
- pervasive security "

⇒ Model for Network Security.

11/8/22

- Passive attacks are very difficult to detect as attacker is not modifying the real data.

Ex :- 1. reading the message contents
2. traffic analysis.

- But Protocol layer is designed such that it prevents passive attacks using cryptography. such that the data is in unreadable format.

- Types of active attacks:
  1. masquerade
  2. replaying
  3. modifying the msg content
  4. denial of service

- We cannot prevent active attacks completely but can be detected where & how abt attacks.

- Masquerade : Msg is not being modified.
The opponent reads the msg & sends to the receiver as the intending users. [pretending as the sender] the receiver doesn't realise the msg is coming from the opportunity.

- Replaying : replaying same msg in some other session [no modifican in content].

3. Modify either a part or whole msg.

4. denial of service : Attacker attacks the communica channel such that there will not be any communican between the intended users.

Security concepts

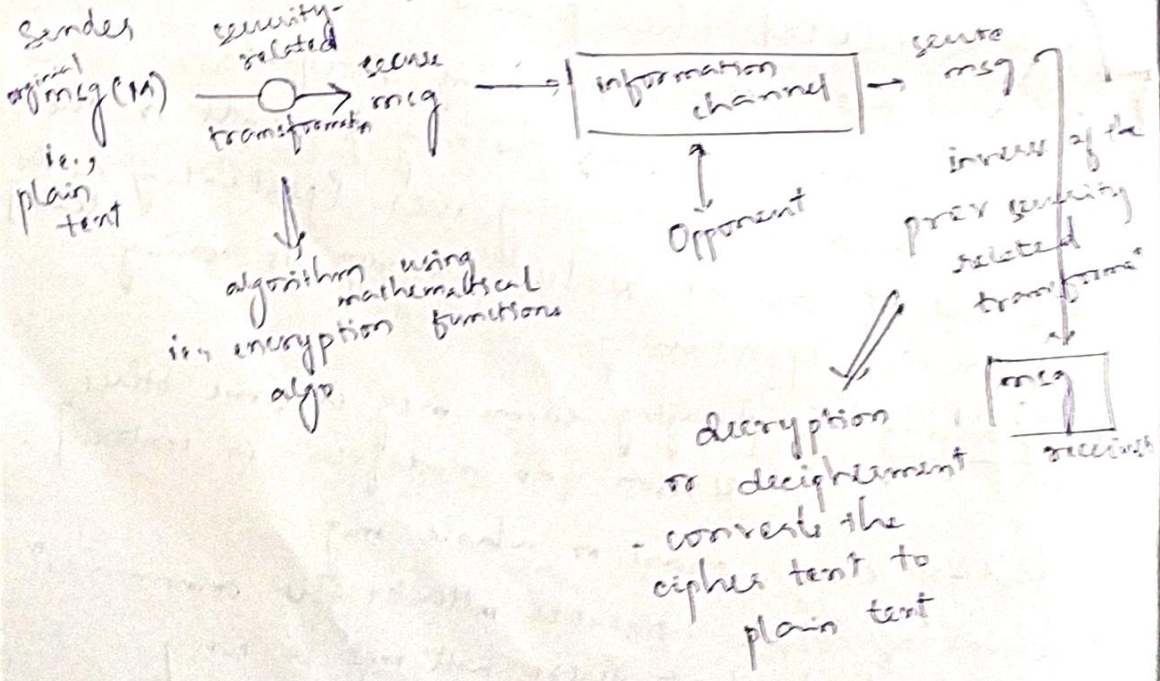
1. data confidentiality → data is not tampered during transmission
2. data integrity
3. data availability.
   - data should be made available to the authorized users.
   - even after a security breach.
4. data authenticity
5. accountability.
   - maintaining records of the actions of the entities
   - assurance to the sender that the msg is received same as the what sender sent.

A → B

4. Authentication: B should be proved A has sent it.
   Only the intended authenticated user should send it.

Model for Network Security:

third party → shares the key between the sender & receiver.



Security related to information — encryption → encipherment

secure msg - or cipher text

Security Mechanisms:

1. Specific security mechanisms provides services to particular architecture
Generally TCP/IP or OSI architecture.
the security service X.800: provided at protocol layer of communication channel.

* Data Authentication:-
  - Peer entity authentication
  - data-origin authentication.

Peer entity authentication → provides both parties authenticity

data-origin authentication → only the intended party is sending data. i.e., ensures receiver.

Access Control:
provides access to only authorized users.
Provided by OSI architecture
Prevents the unauthorized use of resources.

Data Confidentiality:
- connection confidentiality → all data confidentiality assured.
- connectionless confidentiality → confidentiality assured for some all user data in a single data block.
- Selective-field "
- Traffic-flow "

Data Integrity:
- connection integrity with recovery.
- connection " without recovery
- selective field connection integrity
- connectionless integrity
- selective field connectionless integrity.

Non repudiation :

- non repudiation origin
- " destination.

both parties cannot deny the fact

the sender cannot deny that he sent the msg after he sent

the receiver cannot deny the fact that he received the msg after he received the msg.

17/8/22 Security Mechanisms : → Specific Security Mec 10 X.800

1. Encipherment (or encryption) - plain text to cypher text
2. Digital Signature - msg appended with signature/ authenticity of source.
3. Access control

To provide various services mentioned under X.800 service, it uses one or more security mechanisms

4. Data Integrity
5. Authentication exchange : Before original communication the sender & receiver exchanges a variety of data blocks to ensure the authenticity/identity of peers
6. Traffic Padding : Insertion of bits into gaps in a data stream to frustate traffic analysis attempts
7. Routing control : After an attack, it allows the sender to physically select secured route
8. Notarization : trusted third parties.

~~7/8/22~~

Pervasive Security Mechanisms (not intended to one particular service but a general case).

- not particular to any (standard) OSI security architecture.

1. Trusted functionality or
2. Security label
3. Event detection
4. Security audit trail
5. Security recovery

- Interconnection between security services & security mec
  ↳ Table.

NUMBER THEORY :

- Divisibility :- $b|a$ if $a = mb$ then a is divisible by b

Modulus : $a \% b$ - remainder of division.

$$a = qb + r$$

In cryptography :

$13|182$ — 13 divides 182. ✓

$-3|33$ — -3 divides 33 ✓

Properties of divisibility :-

→ If $a|1$ then $a = \pm 1$

→ If $a|b$ and $b|a$ then $a = \pm b$

→ Any $b \neq 0$ divides 0. [ie., 0 can be divided by any int]

→ If $a|b$ & $b|c$ then $a|c$.

→ If $b|g$ & $b|h$ then $b|(mg + nh)$

In cryptography :

+ve integers : 1 to n.

non-negative int : 0 to n.

Division Algorithm :

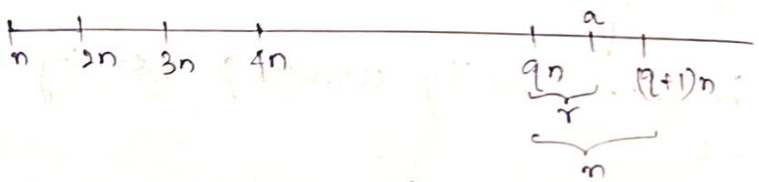
Given any +ve integer 'n'.

Given any non -ve integer 'a'

$$a = q(n) + r \qquad 0 \le r < n$$

$q = \lfloor a/n \rfloor$ → largest int such that a divides n.

On number line:



$a = qn + r$

22/8/22

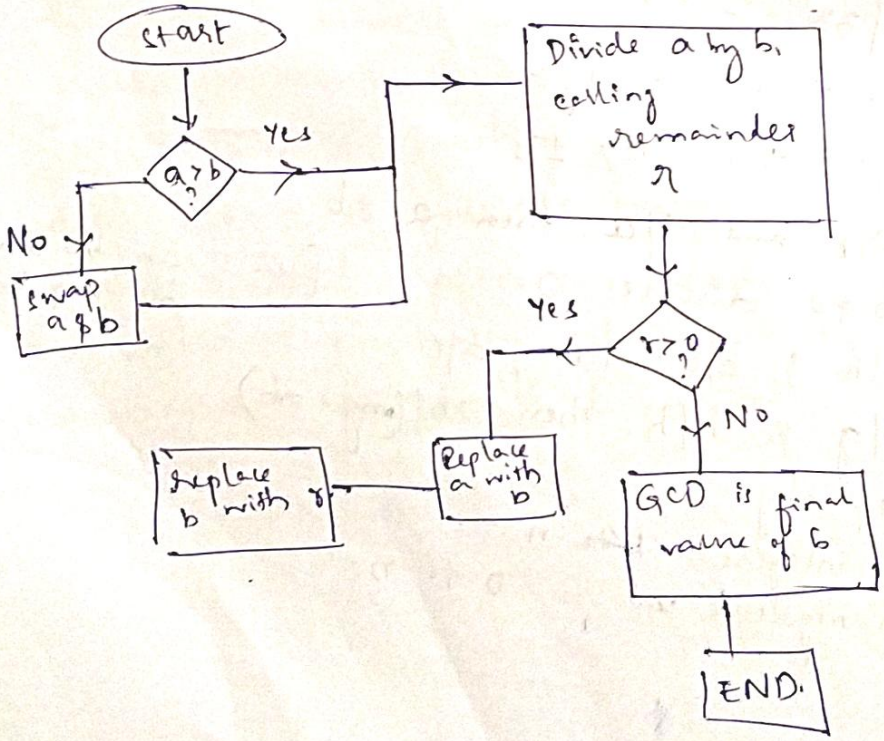
Euclidian Algorithm

GCD (n_1, n_2)

Relatively prime : 2 numbers are said to be relatively prime when GCD of 2 numbers is 1

Ex:- GCD (9,7) = 1

GCD (3,8) = 1



GCD (710, 310)
a b

a > b

710 | 310 q = 2
r = 90

710 = 2 × 310 + 90

r > 0

a = 310 b = 90

310 | 90

310 = 90 × 3 + 40

a = 90 b = 40

90 = 2 × 40 + 10

a = 40 b = 10

40 = 10 × 4 + 0

a = 10 b = 0.

GCD (20, 75)

a < b

swap

a = 75 b = 20

75 | 20 ⇒

75 = 20 × 3 + 15

a = 20 b = 15

20 = 15 × 1 + 5

a = 15 b = 5

15 = 5 × 3 + 0

GCD = 5

$a = q_1 b + r_1 \quad 0 < r_1 < b$

$b = q_2 r_1 + r_2$

$r_1 = q_3 r_2 + r_3 \quad 0 < r_3 < r_2$

$r_{n-2} = q_n r_{n-1} + r_n$

$0 < r_n < r_{n-1}$

$r_{n-1} = q_{n+1} r_n + 0$

gcd (a, b) = r_n

·Recursion function of euclidean algorithm:

gcd (a, b) = gcd (b, a mod b) a > b

euclid (a, b)

if (b = 0) return a

return euclid (b, a mod b)

Ex:- gcd (33, 63) = gcd (63, 33)

gcd (33, 30) → gcd (30, 3) → gcd (3, 0) ⇒ return 3.

Modular Arithmetic :-

a = qb + r

r = a mod b

q = ⌊a/b⌋ largest integer such that a is div by b.

11 mod 5 = 1

-11 mod 5 ⇒ (-11 + 5) mod 5 = -6 mod 5

(-6 + 5) mod 5 ⇒ -1 mod 5 ⇒ (-1 + 5) mod 5

⇓

④ ⇐ 4 mod 5

-23 mod 10 = 7

Congruence : $a \pmod n \equiv b \bmod n$

$73 \bmod 23 = 4$ (a)
$4 \bmod 23 = 4$ (b)

$73 \equiv 4 \bmod 23$ ($\frac{a}{a} \equiv \frac{b}{b} \bmod \frac{n}{n}$)

$73 \equiv 27 \bmod 23$

$73 \bmod 23 = 4$
$27 \bmod 23 = 4$

$73 \equiv 4 \bmod 23$

~~$73 \bmod 23 = 4$~~

if $a \equiv 0 \pmod n$ then $n \mid a$

Properties of congruencies :

1. $a \equiv b \pmod n$ if $n \mid (a-b)$
2. $a \equiv b \bmod n$ implies $b \equiv a \bmod n$
3. if $a \equiv b \bmod n$ & $b = c \bmod n \Rightarrow a = c \bmod n$

$(a \bmod n + b \bmod n) \bmod n = (a+b) \bmod n$.

$(11 \bmod 8 + 15 \bmod 8) \bmod 8 = (11+15) \bmod 8$.

$(3+7) \bmod 8$ 2

$(a \bmod n - b \bmod n) \bmod n = (a-b) \bmod n$

$(a \bmod n * b \bmod n) \bmod n = (a*b) \bmod n$

Ex:- $(11 \bmod 8 * 15 \bmod 8) \bmod 8 = (11 * 15) \bmod 8$

$(3 * 7) \bmod 8 = 165 \bmod 8$.

$21 \bmod 8$ 5

5

Exponentiation : $11^7 \bmod 13$

$11 \bmod 13 = 11$

$11^2 \bmod 13 = 9$

$11^4 \bmod 13 = (11^2 \cdot 11^2) \bmod 13$

$= (9 \times 9) \bmod 13$

$= 3$

$11^7 \bmod 13 = (11 \cdot 11^2 \cdot 11^4) \bmod 13$

$= (11 \times 9 \times 3) \bmod 13$

$= 132 \bmod 13 = 2$

$(x+y) \bmod n = 0$

$x \quad y$

$x \bmod n$

$y \bmod n$

$n = 8$

$x = 0$	8
$x = 1$	7
$x = 2$	6
$x = 3$	5
$x = 4$	4

} Additive inverse.

$(x \times y) \bmod n = 1 \Rightarrow$ multiplicative inverse

$Z_n = (0 \text{ to } n-1) \ldots$

$x = 0$ —

$x = 1 \times 1 \bmod 8 = 1$

$x = 2 \times \_ \bmod 8 = \_$

$x = 3 \times 3 \bmod 8 = 1$

$= 4 \times \_ \bmod 8 = \_$

$= 5 \times 5 \bmod 8 = 1$

$= 6 \times \_ \bmod 8 = 1$

$= 7 \times 7 \bmod 8 = 1$

$x = 11$

$x = 0$ —

$x = 1 \times \_ \bmod 11 = 1$

$= 2 \times 6 \bmod 11 = 1$

$= 3 \times \_ \bmod 11 = \_$

$= 4 \times 3 \bmod 11 = 1$

$= 5 \times 9 \bmod 11 = 1$

$= 6 \times 2 \bmod 11 = 1$

$= 7 \times 8 \bmod 11 = 1$

$= 8 \times 7 \bmod 11 = 1$

$= 9 \times 5 \bmod 11 = 1$

$= 10 \times 10 \bmod 11 = 1$

23/8/22 Extended Euclidean Algorithm:

$d = \gcd(a,b)$ $a > b$ — d expressed as linear combination of a,b

then $d = ax + by$: x, y integer coefficients

d expressed in euclidean algo.

gcd (1547, 560)

$1547 = 2 \times 560 + 427$

$560 = 1 \cdot 427 + 133$

$427 = 3 \cdot 133 + 28$

$133 = 4 \cdot 28 + 21$

$28 = 1 \cdot 21 + 7$

$21 = 3 \cdot (7) + 0$

↑ GCD.

$7 = 1547(x) + 560y$. Find x, y using extended euclidean algo.

Trace back

$7 = 28 - 1 \cdot 21$

$7 = 28 - 1[133 - 4(28)]$

$7 = 5 \cdot 28 - 1 \cdot 133$

$7 = 5(427 - 3 \cdot 133) - 1 \cdot 133$

$7 = 5 \cdot 427 - 16 \cdot 133$

$7 = 5 \cdot 427 - 16(560 - 1 \cdot 427)$

$7 = 21 \cdot 427 - 16 \cdot 560$.

$7 = 21(1547 - 2 \cdot 560) - 16 \cdot 560$.

$7 = 21(1547) - 58(560)$

$d = x(a) + y(b)$

$x = 21 \quad y = -58$

Euclidean algorithm

$q_1 = \lfloor a/b \rfloor$

$r_1 = a \bmod b$.

$a = q_1 b + r_1$

$r_2 = b \bmod r_1$, $b = q_2 r_1 + r_2$

$r_3 = r_1 \bmod r_2$.

$r_n = r_{n-2} \bmod r_{n-1}$

$r_{n+1} = r_{n-1} \bmod r_n$

will = 0.

Extended Euclidean algo.

r_{-1}

r_0

Extended Euclidean Algo

i	calculate			
-1	$r_{-1} = a$	$x_{-1} = 1$	$y_{-1} = 0$	Initialize
0	$r_0 = b$	$x_0 = 0$	$y_0 = 1$	
1	$r_1 = a \bmod b$ $q_1 = \lfloor a/b \rfloor$	$x_1 = x_{-1} - q_1 x_0$	$y_1 = y_{-1} - q_1 y_0$	
2	$r_2 = b \bmod r_1$ $q_2 = \lfloor b/r_1 \rfloor$	$x_2 = x_0 - q_2 x_1$	$y_2 = y_0 - q_2 y_1$	

Repeat till we find $r_n = 0$

$r_n = r_{n-2} \bmod r_{n-1}$ $\quad x_n = x_{n-2} - q_n(x_{n-1})$

$q_n = \lfloor r_{n-2} / r_{n-1} \rfloor$ $\quad y_n = y_{n-2} - q_n y_{n-1}$

where $r_n = 0$.

i.e., $r_{n+1} = r_{n-1} \bmod (r_n) = 0$

↓

gcd.

Ex:- Find the gcd (1759, 550) & find x, y.

i	r_i	q_i	x_i	y_i
-1	1759		1	0
0	550		0	1
1	109	3	$1-3(0)$ $=1$	$0-1(3)$ $=-3$
2	$550 \% 109$ 5	$\lfloor 550/109 \rfloor = 5$	$0-5(1)$ $=-5$	$1-(-3(5))$ $=16$
3	$109 \% 5$ 4	$\lfloor 109/5 \rfloor = 21$	$1+106$ $=+106$	-339
4	$5 \% 4$ 1 gcd	1	-111	355
5	0	4		

So, $1 = -111(1759) + 355(550)$

• For each of the following equations, find value of x

(i) $3x \equiv 4 \pmod 5$ $3x \bmod 5 = 4 \bmod 5$ $x = 3$ $9 \bmod 5 = 4$

(ii) $9x \equiv 3 \pmod 7$ $9x \bmod 7 = 3 \Rightarrow x = 5$ $45 \bmod 7 = 3$

(iii) $7x \equiv 6 \pmod 9$ $7x \bmod 9 = 6 \Rightarrow x =$

• Find gcd of 2740 & 1760 using extended euclidean algo.

i	x_i	q_i	x_i	y_i
-1	2740		1	0
0	1760		0	1
1	980	1	$1-1(0)$ $=1$	$0-1(1)$ $=-1$
2	780	1	$0-1(1)$ $=-1$	$1-1(-1)$ $=2$
3	200	1	$1-1(-1)$ $=2$	$-1-1(2)$ $=-3$
4	180	3	$-1-3(2)$ $=-7$	$2-3(-3)$ $=11$
5	20	1	$2-1(-7)$ $=9$	$-3-11$ $=-14$
6	0	9		

$9(2740) - 14(1760) = 20$

26/8/22 Prime Numbers

$p \rightarrow \pm 1, \pm p$ are divisors

$a = p_1^{a_1} \times p_2^{a_2} \times \cdots \times p_n^{a_n}$ → prime factorisation. (a - integer)

$19 = 2^1 \times 7^1$

$15 = 3^1 \times 5^1$

$28 = 2^2 \times 7$

P is a set of prime numbers then any integer a can be expressed as

$$a = \prod_{p \in P} p^{a_p} \quad \text{where each } a_p \geq 0.$$

- Multiplication of two numbers

$216 = 2^3 \times 3^3$

$300 = 2^2 \times 3^1 \times 5^1$

$18 = 2^1 \times 3^2 \times 5^0$ (get min)

$\gcd(300, 18) = 2^1 \times 3^1 \times 5^0 = 6.$

$k = \gcd(a, b)$

then $k_p = \min(a_p, b_p)$ for all p.

Fermat's Theorem :

If p is a prime number, & a is an integer not divisible by p, then $a^{p-1} \equiv 1 \bmod p$

Alternative form: $a^p \equiv a \bmod p$

a should be relatively prime to p.

no need of a & p being relatively prime

a = 7 p = 19

$7^{18} \equiv 1 \bmod 19$

$7^{19} \equiv 17 \bmod 19$

Euler's totient function : $\phi(n)$

= is the no. of numbers < n & relatively prime to n

⇓

if gcd of two numbers = 1

n = 5, $\phi(n) = \{1, 2, 3, 4\} = 4$

$\phi(n) = n-1$ if n is a prime number

$\phi(11) = 10$ $\phi(7) = 6$

for non-prime,

$\phi(8) = \{1, 3, 5, 7\} = 4$

$\phi(14) = \{1, 3, 5, 9, 11, 13\} = 6$

- two prime numbers p, q ($p \neq q$)

$n = pq$

$\phi(n) = \phi(p) \cdot \phi(q)$

$\phi(n) = (p-1)(q-1)$

Ex:- p = 2 q = 7

$\phi(14) = 1(6) = 6$

Euler's theorem :

For every a and n that are relatively prime to each other, $a^{\phi(n)} \equiv 1 \pmod{n}$.

alternate form: $a^{\phi(n)+1} \equiv a \pmod{n}$

a*5

a=3 n=10

$\phi(n) = 1 \times 4 = 4$

$3^4 \bmod 10 = 1$

$3^5 = 3 \bmod 10$

$3^4 \bmod 10 = 1$

$81 \bmod 10 = 1$

Properties of prime numbers :

1. n is an odd integer, n+ve can express $n-1 = 2^k \times q$ q odd again. $k > 0$ & q is odd.

Ex:- $n = 11 \quad 10 = 2 \times 5$

$n = 13 \quad 12 = 2^2 \times 3$

$25 = 2^3 + 1$

$n - 1 = 4$

$16 = 2^4$

2. If p is prime, a is a +ve integer less than p.

then $a^2 \bmod p = 1$ if and only if $a \bmod p = 1$

or $a \bmod p = -1 \bmod p$

$= p-1$

Ex:- p=7 a=6

$6^2 \bmod 7 = 1$ iff $6 \bmod 7 = 1$ (✗)

or $6 \bmod 7 = -1 \bmod 7$

$= 6.$ (✓)

so true

True for only two values of a.

a should be 1 or p-1

If p is a prime number greater than 2

$p-1 = 2^k q$ with $k>0$, q odd

Let a be an integer $1 < a < p-1$ then one of the following conditions is true

1. $a^q \equiv 1 \bmod p$
2. one of the numbers

$$a^q, a^{2q}, a^{4q} \ldots a^{2^{k-1}q} \equiv -1 \bmod p = p-1$$

$1 \le j \le k$ $\quad a^{2^{j-1}q} \equiv -1 \bmod p = p-1$

Rabin miller algo

- If above two conditions 1, 2 hold, then p may be prime

Rabin Miller Algo:

Test(n)

Find integer k, q with $k>0$, q odd such that

$n-1 = 2^k q$.

Select a random integer $1 < a < n-1$

if $a^q \bmod n = 1$ then return ("inconclusive")

for $j = 0$ to $k-1$ do

if $a^{2^j q} \bmod n = n-1$ then return ("inconclusive")

return ("composite").

Iteratively do for all a: If returns composite ⇒ yes else may not be prime

Eg:- $n = 2047$, $a = 2$ → check

$= 23 \times 89$

$2046 = 2^k \cdot q$

$= 2 \times 1023$ $\quad k = 1$, $q = 1023$

$a = 2$

$2^{1023} \bmod 2047 = 1$ ⇒ true hence return (inconclusive)

i.e., says may be prime

but in real it is composite.

Residue classes

of all integers in a residue class, the smallest non-ve int is one usually used to represent the class.

Finding smallest non-ve integer to which it is congruent modulo n is called reducing b modulo n

$(a+b) \equiv (a+c) \bmod n$

$\Downarrow$

$b \equiv c \bmod n$

For each $w \in Z_n$, there exists a z such that $w+z \equiv 0 \bmod n$

if $(a \times b) \equiv (a \times c) \bmod n$ then $b \equiv c \bmod n$

if a is relatively prime to n.

$\Downarrow$

two integers are relatively prime iff their only common +ve integer factor is 1.

30/3/22

Residue classes mod n :

$Z_n = \{0 \dots n-1\}$ (set of residues or residue classes mod n)

$[0]\ [1] \dots [n-1]$ where

$[x] = \{a : a \text{ is an integer}; a \equiv x \bmod n\}$ ($a \bmod n = x \bmod n$)

The residue classes mod 4 are

$[0] = \{\dots -16, -12, -8, -4, 0, 4, 8, 12, 16, \dots\}$

$[1] = \{\dots -15, -11, -7, -3, 1, 5, 9, 13, 17 \dots\}$

$[2] = \{\dots, -14, -10, -6, -2, 2, 6, 10, 14, 18 \dots\}$

$[3] = \{\dots, -13, -9, -5, -1, 3, 7, 11, 15, 19 \dots\}$

Chinese Remainder Theorem : (CRT)

Any integer can be reconstructed from a pair of integers mod residue classes.

Cond^n :- the residue classes should be relatively prime to each other

Ex:- $x \equiv \underset{a_1}{3} \bmod \underset{\text{mod } 1}{8}$ } relatively prime

$x \equiv \underset{a_2}{3} \bmod \underset{\text{mod } 2}{5}$

x can be reconstructed using 5, 3 or vice versa.

m_1, m_2 relatively prime.

$a_1 = 5 \quad a_2 = 3 \quad m_1 = 8 \quad m_2 = 5$

$M = m_1 \times m_2$

$= 8 \times 5 = 40$

$M_1 = \frac{M}{m_1} = \frac{40}{8} = 5$

$M_2 = \frac{M}{m_2} = \frac{40}{5} = 8$

$x = a_1 M_1 y_1 + a_2 M_2 y_2 \pmod M$

$x = 5(5) y_1 + 3(8) y_2 \pmod{40}$

$M_1 y_1 \equiv 1 \bmod m_1$ $\quad M_2 y_2 \equiv 1 \bmod m_2$

$5y_1 \equiv 1 \bmod 8$ $\quad 8y_2 \equiv 1 \bmod 5$

$y_1 \equiv 5 \bmod 8$ $\quad y_2 \equiv 2 \bmod 5.$

$X = a_1 M_1 y_1 + a_2 M_2 y_2 \pmod M$

$= 5(5)(5) + 3(8)(2) \pmod{40}$

$= (125 + 48) \bmod 40$

$= 173 \bmod 40$

$13 \bmod 40$ < $5 \bmod 8$, $3 \bmod 5$

ie., $X = 13.$

$13 = (5, 3)$

For all the pair of relatively prime residual classes, we can find a pair of numbers from which X can be reconstructed.

Ex:- 973 mod 1813 find a_1, a_2

$973 = (a_1, a_2)$ given $m_1 = 37$, $m_2 = 49$

973 < $a_1 \bmod 37$, $a_2 \bmod 49$

$M = 37 \times 49$

$M_1 = \frac{M}{m_1} = 49 \Rightarrow M_1^{-1} = \_\_\_ \bmod m_1$

multiplicative inverse

$M_2 = \frac{M}{m_2} = 37$ $\quad = \_\_\_ \bmod 37$

$49 \times ?$

$= 34 \bmod 37$

$M_2^{-1} = \_ \bmod m_2$

$= 373^{?} \bmod 49$

$= (4) \bmod 49$

$\downarrow_{-1}$

M_2

$973 = 11 \bmod 37$ $\quad 973 = (11, 42)$

$973 = 42 \bmod 49$

Def:

Let $M = \prod_{i=1}^{k} m_i$

where m_i are relatively prime

i.e., $\gcd(m_i, m_j) = 1 \quad i \neq j$.

Any integer in Z_k can be represented by k-tuple

$A \leftrightarrow (a_1, a_2, \ldots a_k)$

where $A \in Z_M$, $a_i \in Z_{m_i}$ and $a_i = A \bmod m_i$ for $1 \leq i < k$.

Ex:- Use CRT to find

$X = 3 \bmod 7$

$X = 3 \bmod 13$.

$a_1 = 3 \quad a_2 = 3 \quad m_1 = 7 \quad m_2 = 13$

$M = m_1 \times m_2 = 7 \times 13$

$M_1 = 13 \quad M_2 = 7$

$X = a_1 M_1 y_1 + a_2 M_2 y_2 \pmod M$

$M_1 y_1 = 1 \bmod m_1$

$13 y_1 \equiv 1 \bmod 7$

$13 M_1 \bmod 7 = 1 \quad y_1 \equiv (6) \bmod 7$

$M_2 y_2 \equiv 1 \bmod m_2$

$7 y_2 \equiv 1 \bmod 13.$

$7 y_2 \bmod 13 = 1$

$y_2 = 2 \bmod 13$

$x = 3 \times 13 \times 6 + 3 \times 7 \times 2 \pmod{91}$

$= 276 \bmod 91$

$3 \bmod 91$

$x = 3//$

Discrete logarithms :

$Z_n = \{$ the collection of numbers that are relatively prime to $n\}$

$Z_{14} = \{1, 3, 5, 9, 11, 13\}$

Given,

1, $n = 2, 4, p^k, 2 \cdot p^k$ for $k \in N$ and p is odd prime

2, Given $\alpha \in Z_n^*$ is a generator

3, $\beta \in Z_n^*$ (not necessarily a generator)

Compute $\log_\alpha \beta$ i.e., find x such that $\alpha^x \equiv \beta \bmod n$

α is a generator of Z_n if, [$\phi(n)$ - no. of elements in Z_n]

from $\alpha^0 \bmod n$ .... $\alpha^{\phi(n)-1} \bmod n$ should yield all numbers in Z_n.

If α is not a generator, there doesnot exist logarithm.

Eg:- Given $n = 9$ $p^k = 3^2$ α^0 to α^5

$Z_9 = \{1, 2, 4, 5, 7, 8\}$

$\phi(n) = 6$

Let $\alpha = 2$ → $2^0 \bmod 9 = 1$ → $0 = \log_2^1$

$2^1 \bmod 9 = 2$ → $1 = \log_2^2$

$2^2 \bmod 9 = 4$ → $2 = \log_2^4$

$2^3 \bmod 9 = 8$ → $3 = \log_2^8$

$2^4 \bmod 9 = 7$ → $\log_2^7 = 4$ because $2^4 = 7 \bmod 9$

$2^5 \bmod 9 = 5$

So, α is a generator.

$\log_2^7 = x$ (x)

$2^x \equiv 7 \bmod 9$

$\equiv 7$

$\alpha = 4$

$4^0 \bmod 9 = 1$

$4^1 \bmod 9 = 4$

$4^2 \bmod 9 = 7$

$4^3 \bmod 9 = 1$

$4^4 \bmod 9 = 4$

4 is not a generator

$\alpha = 5$ $5^0 \bmod 9 = 1$

$5^1 \bmod 9 = 5$

$5^2 \bmod 9 = 7$

$5^3 \bmod 9 = 8$

$5^4 \bmod 9 = 4$

$5^5 \bmod 9 = 2$.

5 is a generator.

cogarithm	0	1	2	3	4	5
number	1	2	4			

Z_p p is prime

$\{1 \ldots p-1\}$

are relatively prime to p.

$a = \log_{\alpha}^{\beta}$ or $\alpha^a = \beta \bmod p$

if α is generator -

$\alpha^0 \bmod p$

$\vdots$

$\alpha^{p-1} \bmod p$

} should generate $1 \ldots p-1$

generator also called as primitive

5/9/22

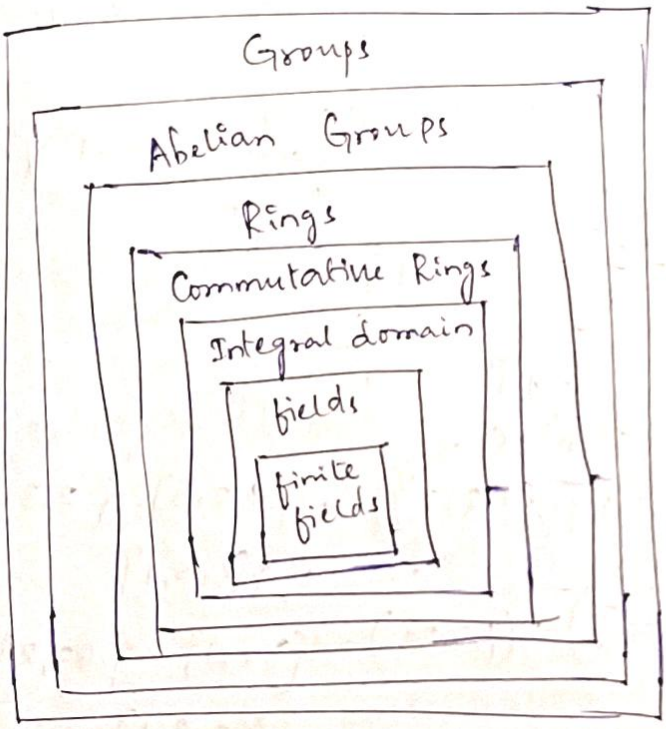


fig 5.2

finite fields are a special fields + some extra axioms

Groups :

denoted by $\{G, \cdot\}$ is a set of elements with binary operation $(\cdot)$ → limited to addition not multiplication

(a, b) ordered pair, $a \cdot b$

A_1 : If a and $b \in G$, then $a \cdot b$ belongs to G

A_2 : $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ $\forall$ a, b, c in G.

A_3 : Identity element : there is an element e in G such that $a \cdot e = e \cdot a = a$ $\forall$ $a \in G$

A_4 : Inverse element : for each a in G there is an inverse a' such that $a \cdot a' = a' \cdot a = e$

Finite groups - elements in a group are finite

vs infinite groups.

Abelian groups :

[Apart from 4 axioms of groups..]

A_5 : Commutative : $a \cdot b = b \cdot a \quad \forall \; a, b \in G$.

Ex:- binary operation is permutation.

$G = \{1, 2, 3\}$

A_1: $\{3, 2, 1\} \cdot \{1, 3, 2\} = \{2, 3, 1\}$

($\{3, 2, 1\}$: permutation elements of grp; $\{1, 3, 2\}$: second element of grp; $\{2, 3, 1\}$: third element of grp)

A_2 : $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

$\{1, 2, 3\} \cdot (\{3, 2, 1\} \cdot \{1, 3, 2\}) = \{1, 2, 3\} \cdot \{2, 3, 1\}$

$= \{2, 3, 1\}$

$(\{1, 2, 3\} \cdot \{3, 2, 1\}) \cdot \{1, 3, 2\} = \{3, 2, 1\} \cdot \{1, 3, 2\}$

$\cdot \{2, 3, 1\}$

A_3 : $a \cdot e = e \cdot a = a$

$a \cdot \{1, 2, 3\} = \{1, 2, 3\} \cdot a = a$ i.e., $e = \{1, 2, 3 \ldots n\}$

A_4 : Inverse : $a \cdot a' = a' \cdot a = e$

$1, 2, 3 \cdot 3, 2, 1$ (inverse)

$3, 2, 1 \cdot 1, 2, 3$

$3, 2, 1$

$3, 2, 1 \rightarrow e$

permutation is group but is not Abelian group.

Cyclic Groups :

A group is called cyclic if every element in G is a power of a^k (k is an integer)

a is a fixed element in G.

a - generator or primitive root of the group

group G should have 'a' such that a^k for $a^k \bmod n$ should be able to produce all elements in G. → no. of elements in grp.

$Z_5 = \{0, 1, 2, 3, 4\}$ $n = 5$

$a = 2$

$2^0 \bmod 5$

$2^1 \bmod 5$

$2^2 \bmod 5$

$2^3 \bmod 5$

$2^4 \bmod 5$

till 2^{5-1}

Rings : $\{R, +, \times\}$

→ closure, associativity

A_1 to A_5

Abelian + extra axioms

M_1 : closure under multiplication

If a and $b \in R$, then $axb \in R$.

M_2 : Associativity of multiplication,

$a(bc) = (ab)c$

M_3 : Distributive laws : $a(b+c) = ab + ac \quad \forall\ a, b, c$

$(a+b)c = ac + bc \quad \forall\ a, b, c$

→ A_1-A_5 : R is an Abelian grp wrt addition i.e., R satisfies axioms A_1-A_5 for the additive grp.

Commutative Rings :

M_4 : Commutativity of multiplication

$ab = ba \quad \forall$

$a, b \in R$

Number theory + finite fields

7/9/22

Rings : (A1 - M6)

- Commutative Rings :

M4 : Commutativity of multiplication

$ab = ba$

* Integral Domain

Commutative Ring + these axioms.

M5 : Multiplicative identity : there is an element 1 in R such that $a1 = 1a = a \ \forall \ a \in R$.

M6 : No zero divisors

If $a, b \in R$ & $ab = 0$ then $a = 0$ or $b = 0$.

Ex :- $\mathbb{Z}$ is an integral domain.

Fields :-

Typical fields : Binary fields.

Quotient of polynomial mod 2.

F denoted by $\mathbb{F}\{F, +, \times\}$

$\forall \ a, b, c \in F$,

integral domain + these axioms.

(A1 - M6)

M7 : Multiplicative inverse : $\forall \ a \in F$ (except 0),

$\exists \ \bar{a} \in F$ such that

$a\bar{a}^{-1} = (\bar{a}^{-1})a = 1$

Ex :- $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields.

Arithmetic on polynomials:

Let R be an arbitary ring. A polynomial over R is an expression of the form.

$$f = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + \cdots + a_n x^n$$

Type-1 fields : Normal polynomial
coefficients can be anything

Type-2 " : coefficients represented by 0/1
ie., coff mod 2.

Ex:- $f(x) = x^3 + x^2 + 2$ $\quad g(x) = x^2 - x + 1$

$f(x) + g(x) = x^3 + 2x^2 - x + 3$

$f(x) - g(x) = x^3 + x + 1$

$f(x) * g(x) = x^5 + 3x^2 - 2x + 2$

} Type-1 arithmetic

Type-2 arithmetic :
arithmetic on the coff is performed mod p
in type 2. p=2 ie., GF(2).

Type-3 : coff's are calculated mod some other polynomial $m(x)$ whose highest power is n

Ex:- GF(2)

$f(x) = x^7 + x^5 + x^4 + x^3 + x + 1$

$g(x) = x^3 + x + 1$

Add : $x^7 + x^5 + x^4$

Sub : $x^7 + x^5 + x^4$

Mul : $x^{10} + x^4 + x^2 + 1$

Div : quotient : $x^4 + 1$
remainder :

GCD & inverse on type-2 polynomials

We say that polynomial $g \in F[x]$ (field) divides $f \in F[x]$ if there exists a polynomial $h \in F[x]$ such that $f = gh$.

Division theorem :

$$f = qg + r \quad \deg(r) < \deg(g)$$

f, g & polynomials in field F[x]

7/9/22

GF(2) : $F = (Z_{p_1}, +, \times)$

+	0	1
0	0	1
1	1	0

XOR operation

×	0	1
0	0	0
1	0	1

AND operation

Type 3 :-

GF(2^n) : coefficients are calculated mod m(x)

m(x) - irreducible polynomial. which cannot be reduced any further. ie., cannot be factorized any more with degree less than highest deg of m(x).

GF(2^3) ie., n = 3

irreducible polynomial of order 3

$m(x) : x^3 + x + 1$

$f(x) : x^2 + x + 1 \longrightarrow 111$ ie., 7

$g(x) : x^2 + 1 \longrightarrow 101$ ie., 5

1 0 1

$f(x) + g(x) = x^2 + x + 1 + x^2 + 1$

$= 2x^2 + x + 2$ (coef mod 2)

$= 0x^2 + x + 0$

$= x$ i.e., $010 = 2$

$= 2$

addition is same as that of GF(2) when multiplicn degree exceeds of mod $m(x)$ it req.

0 -	0 0 0	0
1 -	0 0 1	1
2 -	0 1 0	x
3 -	0 1 1	$x+1$
4 -	1 0 0	x^2
5 -	1 0 1	x^2+1
6 -	1 1 0	x^2+x
7 -	1 1 1	x^2+x+1

$7 + 5$ in $GF(2^3)$ is 2.

$f(x) \times g(x) = (x^2 + x + 1) \cdot (x^2 + 1)$

$= x^4 + x^2 + x^3 + x + x^2 + 1$

$= x^4 + x^3 + 2x^2 + x + 1$ mod 2

$= x^4 + x^3 + x + 1 \pmod{x^3 + x + 1}$

$$\begin{array}{r} x+1 \\ x^3+x+1 \overline{)\ x^4 + x^3 + x + 1} \\ \underline{x^4 + \ \ + x^2 + x} \\ \ \ \ x^3 + x^2 + 1 \\ \underline{x^3 \ \ + x + 1} \\ -x^2 - x \pmod 2 \end{array}$$

Remainder: $-x^2 - x$.

$(x^3 - x^2 + 1) \bmod 2 \Rightarrow x^3 + x^2 + 1$

$+ x^3 + x + 1$

$-x^2 - x \pmod 2$

$x^2 + x$

$= -x^2 - x \pmod 2$

$= x^2 + x \Rightarrow 6$

In $GF(2^n)$ consider irreplacable polynomial $m(x)$ of degn.

i.e., 7×5 in $GF(2^3)$ is 6.

Addition & subtraction has no diff for GF(2) & $GF(2^n)$.

- How $GF(2^3)$ is advantageous than $GF(2)$?

Mod 8 (Z_8)

×	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)

⇓

Here only some have multiplicative inverses

- Frequency of elements is not uniformly distributed

$GF(2^3)$ ⇒ with using irreducible x^3+x+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	3	(1)	7	5
3	0	3	6	5	7	4	(1)	2
4	0	4	3	7	6	2	5	(1)
5	0	5	(1)	4	2	7	3	6
6	0	6	7	(1)	5	3	2	4
7	0	7	5	2	(1)	6	4	3

⇓

Here we can find multiplicative inverses for all ~~numbers~~ elements in 2^3.

- All elements will be uniformly distributed.

integer	0	1	2	3	4	5	6	7
freq in Z_8		4	8	4	12	4	8	4
freq in $GF(2^3)$		7	7	7	7	7	7	7

non-uniform distribn in GF(8)

Because of this, the most freq elements / patterns can be easily analysed / found by crypto analysts

CRT - Chinese Remainder Theorem example

→ $x \equiv 1 \mod 5$ (a1, mod m1)

$x \equiv 1 \mod 7$ (a2, m2)

$x \equiv 3 \mod 11$ (a3, m3)

$M = 5 \times 7 \times 11 = 35 \times 11 = 385$

$M_1 = \frac{M}{m_1} = 7 \times 11 = 77$

$M_2 = \frac{M}{m_2} = 55$

$M_3 = \frac{M}{m_3} = 35$

$M_1 y_1 = 1 \mod m_1$

$77 (y_1) = 1 \mod 5 \Rightarrow 2 \times 2 = 1 \mod 5$

$77 y_1 \mod 5 = 1$

$y_1 = 3$

$M_2 y_2 = 1 \mod m_2$

$55 y_2 = 1 \mod 7$

$6 y_2 = 1 \mod 7$

$y_2 = 6$

$M_3 \times 3 = 1 \mod 11$

$35 M_3 = 1 \mod 11$

$2 Y_3 = 1 \mod 11$

$Y_3 = 6.$

$X = a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 Y_3 \pmod M$

↓ mod 385

$X = 1(77)(3) + 1(55)(6) + 3(35)(6)$

$= 1191 \mod 385$

$X = 36$

Ex:- $x \equiv 3 \mod 7$

$x \equiv 3 \mod 13$

$x \equiv 0 \mod 12$

$M = 7 \times 13 \times 12 = 1092$

$M_1 = 13 \times 12 = 156$

$M_2 = 7 \times 12 = 84$

$M_3 = 7 \times 13 = 91$

$M_1 y_1 = 1 \mod 7$

$156 y_1 = 1 \mod 7$

$2 y_1 = 1 \mod 7$

$2 y_1 \mod 7 = 1$

$y_1 =$ [illegible]

$M_2 y_2 = 1 \mod 13$

$84 y_2 = 1 \mod 13$

$6 y_2 \mod 13 = 1$

$y_2 = 11$