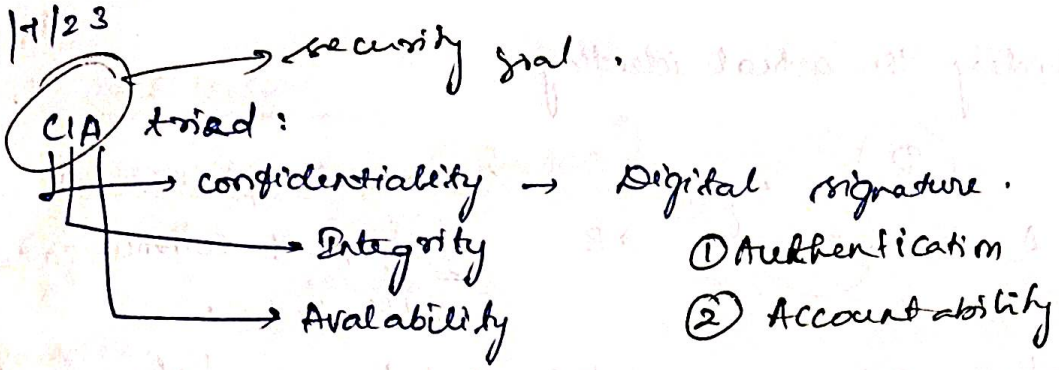
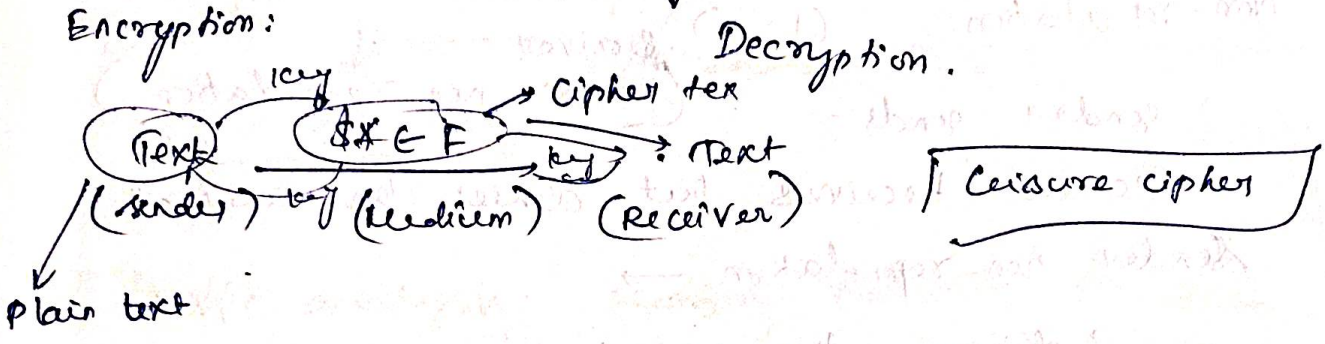
3/1/23



Cryptography



* Symmetric key: for encryption & decryption same key
* Assymmetric key: " " different "

Public key, private key — confidentiality, authentication.

Threat

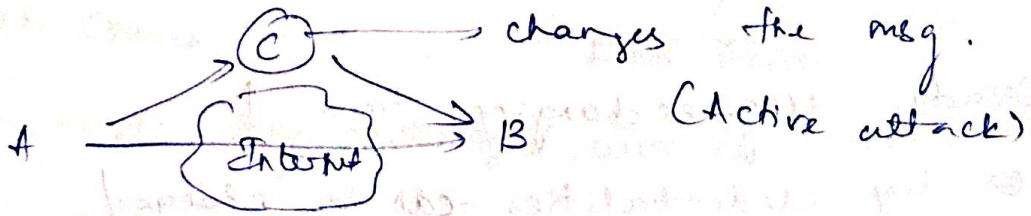
Security Attack: content being read by other

Security mechanism: protecting the msg using algorithm.

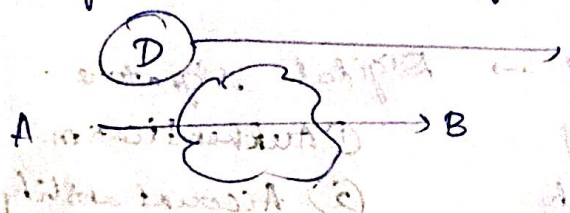
Active attack
↓
Places impact on content modified
#
Integrity of msg is lost

Passive attack
↓
No impact but confidentiality lost.
↓
Eg: Eve's dropping → overhearing
2) Montoring of network traffic

Man in the middle attack:



Mask: Hiding the actual identity.



D masks (pretends) like A & communicates with B.

Integrity, privacy, confidentiality is lost.

Non-reputation: (1:1)

Sender sends

Receiver Receives but denies the receival.

Sender non-repudation → denying the receival of msg

Receiver non-repudation

Authenticity → for trust

Accountability → Responsibility even if flaw in network occurs.

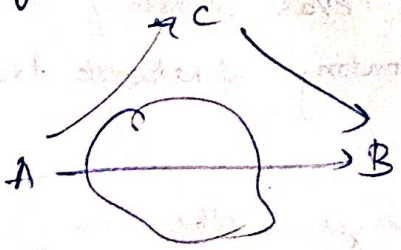
OSI → Open system Interconnection.

OSI for security services:

1) security Attack
2) " Mechanism
3) " services.

DoS → Denial of service → Active attack.

Replay attack: (Replay)



C receives from A without modification & replay to B.

Disadv: Msg exchanging time ↑

Key credentialities can be changed.

1/8/23

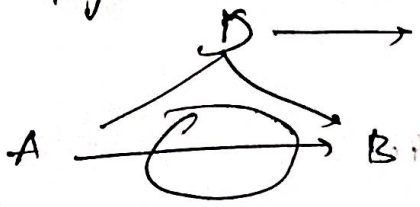
OSI architecture:

1.) security Attack (2marks)
2.) " service
3.) " mechanism

Passive.

Active attack:

1) Snoopy. like eves dropoy



2) Traffic analysis: Monitoring network traffic

Active: 1) Masquerade (Mark)
Mimicing the authorized user to other.

2) Replay: To delay msg transmission.

3) Modification of msg.

4) Repudiation:

DoS:

Unauthorized user keeps the connection to server always open (Tear down doesn't occurs).
due to traffic server can't serve authorized user.

Security services:

1) Authentication
* Peer entity authentication: both sender & receiver
* Data Origin — " Data source.

2) Access ctrl: only authorized user can control.

3) Data confidentiality.

Connection conf : connected users access ✓.
connectionless : IP connection.
Selective field conf : selected field alone accured.
Traffic flow confidentiality : monitoring traffic flow.

Data Integrity :

Non repudiation → origin.
→ Destination

recovery alteration :
Detecting only not Recovery.
connectionless Integrity.
Selective field connection
less

Security Mechanisms :

1. Encipherment → encryption.
2. Data Integrity.
3. Digital Signature
4. Authentication Exchange → Digital key.
5. Traffic Padding
6. Routing ctrl.
7. Notarization → Attestation → Trusted 3rd party.
8. Access ctrl

Pervasive security mechanism : — Not specific to a layer

Setting priority

Trusted func.
Security label
Event detection

Security Audit trail
" Recovery.

8/8/23.

Cryptanalysis

Brute-force attack → passwords (Trial & error)

cryptanalytic attack → strategy to get key using algorithms, plane & cypher text relation, key size.

Kerchoff's principle: Cryptographic System strength → all known, except key - algorithm should be secured.

Plane & cypher text, algorithm.

2m) Types of attack

a) cypher Text only - known to cryptanalyst
full cypher text & encryption algorithm known.

2) known plain Text - combinations of plain text & cypher Text

3) chosen plain Text -

4) " cypher Text

5) " Text

~~Unconditional Secure~~

Brute force search:

↑ key size → ↑ encryption.
↑↓ hardware complexity.

Unconditional security.

Computational " : based on CPU Resource.

Plain text

→ Introduced encryption.

Caesar cipher:

key: 3 → started.

eg: "TEST" encryption

WHVW

@ decryption key = -3.

Q) Encode "spongebob" key = 11.

A	B	C	D	E	F	G	H	I	J	K	L	M	N
0	1	2	3	4	5	6	7	8	9	10	11	12	13
O	P	Q	R	S	T	U	V	W	X	Y	Z		
14	15	16	17	18	19	20	21	22	23	24	25		

SPONGE BOB. — DAZYRTMZM.

cipher text { Plain Text value % 26 → Encryption.
+ key.

key - cipher Text % 26 → decryption.

Cryptanalysis of Caesar cipher

Monoalphabetic cipher: a always F. but for others may change

Poly n : a 1st time F,
2nd time G,
3rd time 2, etc.

→ privilage of mapping char.

~~Play fair cipher:~~

Pervasive security

setting priority security Audit trail

Play fair cipher → Requirements: Plain Text, key

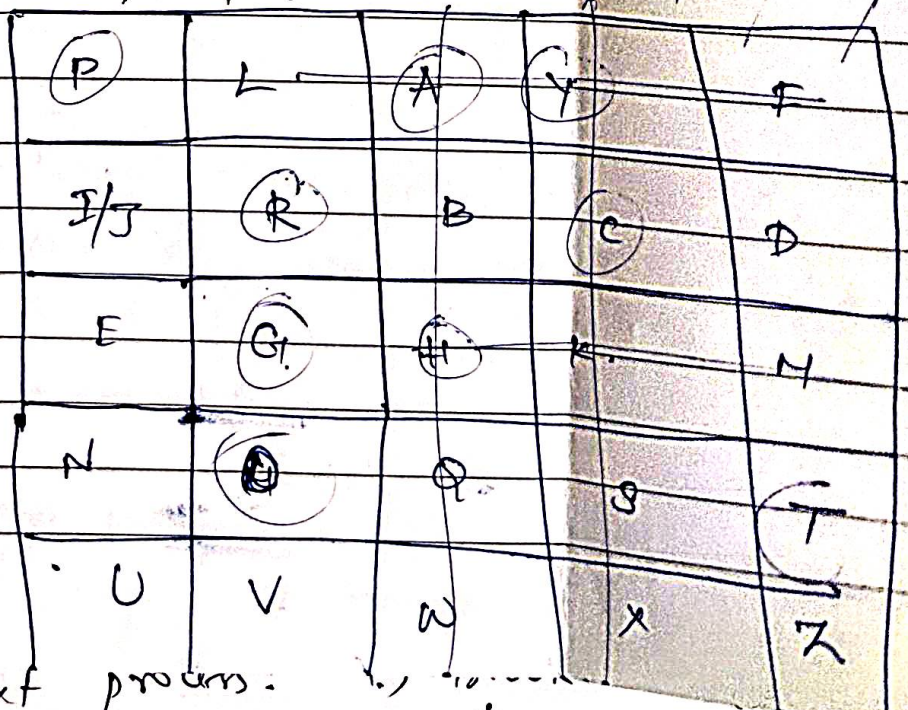
1) BALLOON → plain text
split into 2, no both 2 letters should be same then fill 'x'.
BA/LX/LO/ON.

2. Key: MONARCHY → matrix
play fair cipher → 5x5 matrix, always i & j combined.

1) same column → Replace with below.
2) " row → ~~next~~ replace with next.
3) different both → intersection.
same row but @ col of other pair.

HW Key: play fair plain text: Cryptography.

Cryptography → DB/FL/NQ/OG/YL/KA



Plain text process.

ryption techniques:

Text: msg.

cipher Text: msg (encrypted)

cipher: Encryption.

key: for encrypting & decrypting.

Symmetric — Asymmetric

Cryptography: study of encry. & decryp ... principles

cryptanalysis – codebreaking without key.

Brute force: use trial & error method to open (attack) info.

cryptology = cryptography + analysis.

Symmetric = private = single key.

Asymmetric = public key.

Strong → key
→ Algorithm } = better cipher text.

Cryptography:

- 1.) Substitution – alternating (Replacing)
- 2.) Transposition – changing position
- 3.) Product → Mix

→ Encryption operation.

No. of keys used

1. Single key 2. Public key.

Plain text process: 1.) Block (efficient) eg: password

2.) stream. (each alphabet)

cryptanalysis

of cryptanalytic attack

brute - force attack.

9/8/23

9/8/23 Polyalphabetic ciphers:

→ eg:

Vigenere cipher → Table.

length : key = plain Text
row col.

→ method of polyalphabetical subs.

cipher Text repeation — space

Autokey cipher:

One key till length of PT.

Remain length use PT.

Vernam cipher:

disadv: only binary

One-Time Pad:

auto random key for encryption.

Transposition cipher:

Problem: → Transposition/permutational cipher.

Rail Fence Cipher

in 2 Rails: Meetme.

1st M E M E
2nd E T E

CT: MEMETE.

3 rails.

Row Transposition cipher:

Key: No. of digits.

PT: Arrange in → No. of key digit.

Arrange in ascendig order

Text out in (col out)

PT: Attack postponed until two am.

key: TOMATO
1 2 3 4 5 6

T	O	M	A	T	O
A	T	T	A	C	K
P	O	S	T	P	O
N	E	D	U	N	T
I	L	T	W	O	A
M	Q	X	Y	Z	W
5	3	2	1	6	4

Col out: ATUTW | TSDTX | TOELQ | KOTAW | APNIM

CPNOZ.

Product ciphers:

Combo. of substitution & Transposition. ↑ complexity.

AES, WEP (modem, wifi)

Rotor Machines:

Stegnography: → (Text / Image embedded in Text)
⇓
water marking.

↓
writing img/Text hiding in Text.

Mode of operation:

1. Block & stream cipher:

Block ↓ large volume of data.

stream → key: small size

Block: high diffusion.
multiple encryption iteration } ↑ confusion.

Lom DES

11/8/23

I Electronic code Book (ECB) → independent Block

both encryption & decryption → reverse encryption.

II Cipher block chaining → CBC
→ connection.

IV → initialization vector for 1st block alone.
for further blocks derived.

decryption : CT ⊕ key → Ans ⊕ IV → PT

III Cipher fb (CFB) mode.

(2) ① encrypted IV
↳ ⊕ ← PT
↓
CT

different IV for each block/stream.

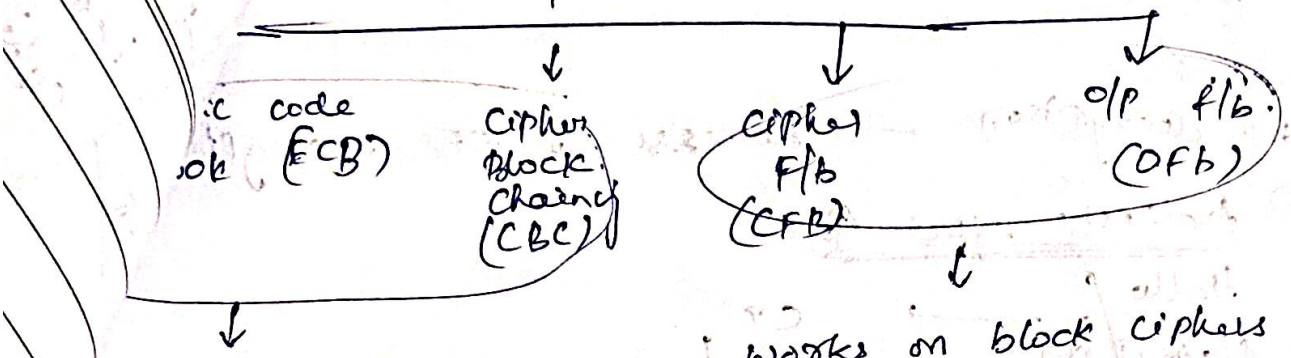
② New IV → shift J bits of CT + IV
↑
shift reg.

IV o/p fb mode (OFB)
use encrypted IV for fb.

V Counter (CTR) mode.
counter in incremental order

Lom description, adv, disadvantage, diag

Algorithm modes



2 blocks works on block ciphers

works on block ciphers acting as stream ciphers.

14/8/23.

DES → Data Encryption Standard. algorithm.

sp network → substitution permutation

↳ both creates complexity

feistel str → many iteration process of plain text to cipher text

clude shannon → proposed sp network

s box p box

to create confusion & diffusion

confusion → key — CT. relation

diffusion → scattered plain text.

key ~~plain text~~ — CT. relation

plain T — CT relation.

Feistal str:

DES → Block cipher

↳ PT = 64 bits.

key: 64 to 56 bits — due to key reduction operation.

16 rounds — each round separate key.

↳ 1.) key transformation — shifts

2.) Expansion permutation → 32 to 48 bits — 8 blocks

3.) S-box permutation

4.) P box permutation.

5.) XOR & Swap.

FAQ (X) DES (or) AES.
1st half

DES decryption → Reverse of DES encryption.

Avalanche effect ↑

Hello / key → CT

Plain T / key → CT → A v. great change.

small change: Hillo / key → CT
PT

Next version of DES → No of keys.

Double, Triple DES

2 keys → Threat @ temp. storage

3 keys → different. ↑ complexity.

(1) K_1, K_2, K_3 → all encryption

(2) (or) K_1, K_2, K_1 → Encryp, Decryp, Encryp

16/8/23.

Qw → 2 or 3 pts.

Criteria for S-box design:

i) No linearity b/w i/p & o/p

ii) 16 possible combinations

iii) 2 i/p, with 1 bit change
o/p: more than 2 bits change

iv) middle bits of 6 bits
4bit

v) 2 1st 2 bits → different
last 2 bits → same
} o/p: different.

vi) non zero — 2 i/ps → 32 pairs
fully different.

Criteria for P box design:

1) S box o/p: 6 bits.

6/5 iterations.

4 bits i/p → impacts next S box.. not on the same S boxes.

2) S_j → change affects S_k

Reverse not possible.

DES design criteria for (F):

→ to create complexity.

→ by creating randomness.

Strict Avalanche criterion: (SAC)

Bit independent criterion (BIC).

↳ change in i/p to o/p — can't trace out.

AES → Advanced Encryption standard

security

cost: implementation in hardware

Flexibility: easy to update, platform independent versatile, simple.

NIST

DES was cracked using high speed computers

triple DES → 3 key → more complex.

slow

small blocks only.

Rijndael — AES (2001)

Criteria for AES

- hardware compatable.
- ↓ space
- overcome attacks.
- Encryption Vs Decryption.
- easy to instal software
- security.
- key agility → size, common/different, strong, generation.

* 9 elements - operations in all levels.

* Versatility & flexibility → platform / version - compatable

Rijndael AES

key: 128 / 192 / 256 bits

Block size: 128 bits.

Round: 10 / 12 / 14.

key length: 16 / 24 / 32 → bytes

Iterative str not Feistel str.

data block: 4 × 4 → bytes. → state matrix.
4 bytes

Operates on entire data block in every round.

* Resistant to attack

* speed ↑, ↑ compactness, compatable

* Simple design.

10 Rounds / # operation
1.) substitute bytes
2.) shift rows
3.) Mix columns → not in last round
4.) Add round key → 8m

Initial transformation → PT → Add round key only occurs.

key: 128 bits in col $W_0, W_1, W_2 \ldots$

→ key expansion.

Substitute bytes → from S box (different from DES)

eg: 95 → col 2A, row

OE → col 76, row

S box — derived from Galois field transformation.
(GF)
Inverse S box
↓
10 polynomials

Shift rows:

1st row → same
2nd " → 1 shift
3rd " → 2 shifts } left.
4th " → 3 shifts

Mix col:

GF polynomial $m(x) = x^8 + x^4 + x^3 + x + 1$

matrix → std. value (Constant)

Inverse mix col → matrix

mixed × Inverse mixed × shift → unity matrix

Add round key:

key: 128 bits

4 bytes → 1 word.

17/8/23.

* for 1st initial transformation use key w (0, 3)
* Then perform key expansion for further rounds from the above ref.
* each round has a const called round const

g has 3 operations

1.) left shift (circular) → Rotate (x)
2.) Sub byte using S box → Sub (y)
3.) Based on round 1 step → ⊕ (y, Round const)
(2)

18/8/23

Unit-2 (Problem)

Number Theory & Public key : Cryptography

Book: cryptography & NS by Behrouz Forouzan

Intro to No theory

cryptographic algorithm → prime no.

∴ breaking key formed using prime no is difficult.

eg: To find prime no.

(1) eg: 97

Sqrt → $\sqrt{97}$ → 9.848 consider only floor

prime no < 9, → 2, 3, 5, 7

97 not divisible by 2, 3, 5, 7

Hence prime no.

(2) 301

$\sqrt{301}$ → 17....

prime no < 17 → 2, 3, 5, (7), 11, 13.

301 ÷ 7 ✓

Hence not prime no.

(3) Euler's phi/Totient func:

Rules:

i) $\phi(1) = 0$

ii) $\phi(p) = p-1$ if p is prime

iii) $\phi(m \times n) = \phi(m) \times \phi(n)$ if m & n are relatively prime

iv) $\phi(p^e) = p^e - p^{e-1}$ if p is a prime

GCD of 2 nos. = 1 (Relatively prime nos)

GCD: (HCF)

1.) 48 & 13.

13 → 1, 13

48 → 1, 2, 3, 4, 6, 8, 12, 24, 48.

→ No other common factor.

GCD (48, 13) = 1. → Relatively prime

2.) 12 & 13

13 → 1, 13

12 → 1, 2, 3, 4, 6, 12

GCD (12, 13) = 1 → RP.

3.) 12 & 15

12 → 1, 2, 3, 4, 6, 12

15 → 1, 3, 5, 15

4.) 36 & 60.

36 → 1, 2, 3, 4, 6, 9, 12, 18, 36.

60 → 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60

Divisibility rule:

2 → 0, 2, 4, 6, 8

3 → Sum of digits divisible by 3

4 → 0, 4

5, → 0, 5

6 → divisible by 2 & 3

8 → 0, 8,

9 → Sum of digits divisible by 9.

10 → 0

11 → difference b/w odd & even digits '0'

or divisible by 11.

Q) $\phi(13) = 13 - 1 = 12$

(13 is prime)

$\phi(p) = p - 1$ if $p \rightarrow$ prime

Q) $\phi(10) = \phi(2 \times 5)$

GCD of 2, 5 : $2 \rightarrow 1, 2$; $5 \rightarrow 1, 5$

2, 5 → Relatively prime ✓

So, $\phi(m \times n) = \phi(m) \times \phi(n)$

$= \phi(2) \times \phi(5)$

$= (2-1) \times (5-1)$

$= 1 \times 4 = 4$

48
2 | 48
2 | 24
2 | 12
2 | 6
3 | 3
1

240
2 | 240
2 | 120
2 | 60
2 | 30
3 | 15
5 | 5
1

Q) $\phi(240)$

LCM of 240 :-

$\phi(2^4 \times (3 \times 5)) = \phi(2^4 - 2^{(4-1)}) \times \phi(3) \times \phi(5)$

$= (16 - 8) \times 2 \times 4$

$= 8 \times 8 = 64$

Another.

$\phi(2^4 \, 3^1 \, 5^1) = (2^4 - 2^3)(3^1 - 3^0)(5^1 - 5^0)$

$= (16 - 8)(3 - 1)(5 - 1)$

$= (8)(2)(4) = 64$

a) $\phi(49) = \phi(7^2)$

$= 7^2 - 7^1 = 49 - 7 = 42$

21/8/23

Q) No. of elements in Z_{14}^*.

Ans: $\phi(14) = \phi(2) \times \phi(7) = 1 \times 6 = 6$ → coprime

Prime Nos: 2, 3, 5, 7, 11, 13.

Fermat's little theorem:

1st version: $a^{p-1} \equiv 1 \bmod p$ → congruence

2nd version: $a^p \equiv a \bmod p$.

$a^{p-1} \bmod p = 1$.

Q) Find the result of $6^{10} \bmod 11$ → $a^{p-1} \equiv 1 \bmod p$

$6^{10} \bmod 11$

$p = 11$ → $p - 1 = 10$

$a = 6$

$1 \bmod (11) = 1 \times 11 = 11$

Q) $3^{12} \bmod 11$

$a^p \equiv a \bmod p \Rightarrow a^p \bmod p = a$

$3(3^{11} \bmod 11) = 3 \times (3) = 9$

Q: $5 \overline{)239}$ (47, 235) → 5×47

4 → remainder

$239 - 5 \times 47$

4 → remainder

2nd) 15/10/8M

Multiplicative inverse (RSA algorithm)

- small nos.
- large nos
- Euclidean Algorithm.

Q) Multiplicative inverse of 8 mod 11 (Q) 25 mod 8)

8 mod 11

8) 11 (1 → quotient
8
3 → Remainder

3) 8 (2
6
2) 3 (1
2
1) 2 (2
2
0

Dividend = Divisor(Quotient) + Remainder

$11 = 8(1) + 3 \Rightarrow 3 = 11 - 8(1)$ ← ③

$8 = 3(2) + 2 \Rightarrow 2 = 8 - 3(2)$ ← ②

$3 = 2(1) + 1 \Rightarrow 1 = 3 - 2(1)$ ← ①

① $\Rightarrow 1 = 3 - 2(1)$

$= 3 - [8 - 3(2)](1)$ ← ②

$= 3 - 8(1) - 3(2)(1)$

$= 3 - 8(1) - 6 = 9 - 8(1)$

$= 3(3) - 8(1)$

→ ③

$= [11 - 8(1)](3) - 8(1)$

$= 11(3) - 8(11(3) - 8(1)$

$= 11(3) - 24 - 8 \quad = 11(3) - 32.$

$= 11(3) - 8(4)$

$= 11(3) + 8(-4)$ → -ve : -4, +ve : 11 − 4 = 7

↓

for 11 mI = 3.

Q) 26 mod 15

11 inverse mod 26.

$5 \overline{)26} \; (5$

25

1

$5 \; (5$

5

0

$11^{-1} \bmod 26$

↓

MI of 11

$26 = 5(5) + 1$

$1 = 25 - 5(5)$

↓

MI of 5 is 5

Q) $-7 \bmod 10$

$8^{-1} \bmod 17$

$5^{-1} \bmod 23$

$60^{-1} \bmod 101$

$22^{-1} \bmod 211$

22/8/23.

Euler's theorem:

1st version: $a^{\phi(n)} \equiv 1 \bmod(n)$

2nd version: $a^{k \times \phi(n)+1} \equiv a \pmod{n}$

Q) find result of $6^{24} \bmod 35$.

$a^{\phi(n)} \equiv 1 \bmod(n)$ $\quad n = 35$

$\phi(35) = \phi(7) \times \phi(5) = 6 \times 4 = 24$

$a^{\phi(35)} \equiv 1 \bmod(35)$

$6^{24} \bmod(35) = 1$

Q) find the result of $20^{82} \bmod 77$.

$n = 77$

$\phi(n) = \phi(7) \times \phi(11)$

$= 6 \times 10 = 60$

2 left out

$(20 \bmod 77)(20^{\phi(77)+1} \bmod 77) \bmod 77$

$(20)(20) \bmod 77$

$20^2 \bmod 77$.

20^2

$77 \overline{)400}$ $\quad 5.1948$

0.1948×77

15

Primality Testing

Deterministic Algorithm → 100% accuracy

Probabilistic Algo → No 100% accuracy

Recommended Primality Test

Deterministic Algo:

1) Divisibility Algo:

2) AKS algo

Probabilistic algorithm:

1) Fermat Test — eqn: If $n \rightarrow$ prime no.

$$a^{n-1} \equiv 1 \bmod n$$

- if $n \rightarrow$ composite possible that $a^{n-1} \equiv 1 \bmod n$.

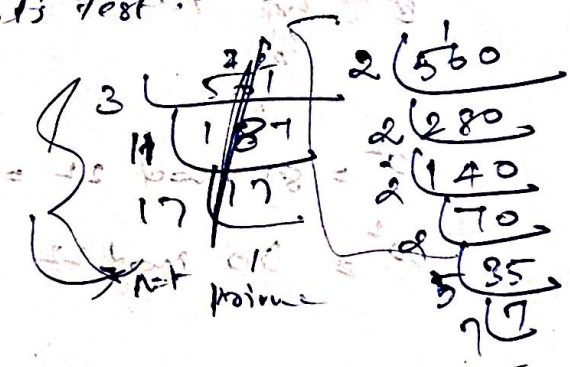
Q) Does the no. 561 pass fermat's test.

Use base $\rightarrow 2$.

$560 = 2^4 \times 5 \times 7$

$a^{n-1} = 1 \bmod n$.

$2^{561-1} = 1 \bmod 561$



Sq. root Test:

Let n → prime : $\therefore \sqrt{1} \bmod n = \pm 1$

→ composite : $\sqrt{1} \bmod n = \pm 1$ possibly other values.

Q) What are the sq. roots of $1 \bmod n$ if n is (a composite)?

$1^2 = 1 \bmod 22$.

$2^2 = 4 \bmod 22$

$3^2 = 9 \bmod 22$

$4^2 = 16 \bmod 22$.

$5^2 = 25 \bmod 22 = 3 \bmod 22$

$6^2 = 36 \bmod 22 = 14 \bmod 22$

$7^2 = 49 \bmod 22 = 5 \bmod 22$.

$8^2 = 64 \bmod 22 = 2 \bmod 22$

$9^2 = 81 \bmod 22 = 5 \bmod 22$.

$10^2 = 100 \bmod 22 = 12 \bmod 22$

Chinese Remainder theorem:

To solve set of congruent eqns.

4 steps

$x \equiv a_1 \pmod{m_1}$

$x \equiv a_2 \pmod{m_2}$

$\vdots$

$x \equiv a_k \pmod{m_k}$

1. $M = m_1 \times m_2 \times \cdots \times m_k$
2. $M_1 = M/m_1, M_2 = M/m_2 \cdots M_k = M/m_k$.
3. Multiplicative inverse $M_1, M_2, \ldots M_k$:

$M_1^{-1}, M_2^{-1}, \ldots M_k^{-1}$

4. $x = (a_1 \times M_1 \times M_1^{-1} + a_2 M_2 M_2^{-1} + \cdots + a_k M_k M_k^{-1}) \bmod M$

Q) $x \equiv 2 \pmod{3}$

$x \equiv 3 \pmod{5}$

$x \equiv 2 \pmod{7}$

① $M = 3 \times 5 \times 7 = 105$

$M_1 = \frac{M}{m_1} = \frac{105}{3} = 35$

$M_2 = \frac{M}{m_2} = \frac{105}{5} = 21$

$M_3 = \frac{M}{m_3} = \frac{105}{7} = 15$

② $M_1^{-1} = 35^{-1} \bmod 3$

$3 \overline{)35} \; (11$

33

2

$\frac{2}{1} \overline{)2} \; (2$

$\frac{2}{0}$

$35 = 3(11) + 2$

$2 = 2(1) + 1$

$1 = 3 - 2(1)$

$1 = 3 - [35 - 3(11)](1)$

$= 3 - 35(1) - 3(11)(1)$

$= 3(12) - 35(1)$

$= 2(12) + 35(-1)$

$3^{-1} \bmod 3$

$3 - 1 = 2$

$M_1^{-1} = 2$

$M_2 = 21^{-1} \bmod 5$

$5 \overline{)} 21 \ (4$

20

$1 \overline{)} 20 \ (20$

20

$0.$

$21 = 5(4) + 1$

$1 = 21(1) - 5(4)$

$M_2^{-1} = 1$

$M_3 = 15^{-1} \bmod 7$

$7 \overline{)} 15 \ (2$

14

$1 \overline{)} 14 \ (14$

14

0

$15 = 7(2) + 1 \Rightarrow 1 = 15(1) - 7(2)$

$M_3^{-1} = 1$

(4) $x = [(2 \times 35 \times 2) + (3 \times 21 \times 1) + (2 \times 15 \times 1)] \bmod 105$

$= [(4 \times 35) + (63) + (30)] \bmod 105$

$= [140 + 63 + 30] \bmod 105$

93

$x = [233] \bmod 105$

$= 23$

$= 23 \bmod 105$

---

(5) $x \equiv 3 \bmod 5$

$x \equiv 1 \bmod 7$

$x \equiv 6 \bmod 8$

(1) $M = m_1 \times m_2 \times m_3 = 5 \times 7 \times 8 = 280$

(2) $M_1 = \frac{M}{m_1} = \frac{280}{5} = 56$

$M_2 = \frac{M}{m_2} = \frac{280}{7} = 40$

$M_3 = \frac{280}{8} = 35$

(3) $M_1^{-1} = 56^{-1} \bmod 5$

$5 \overline{)56} \; (11$

5

$1 \overline{)5} \; (5$

5

0

$56 = 5(11) + 1$

$1 = 56(1) - 5(11)$

$M_1^{-1} = (1)$

$M_2^{-1} = 40^{-1} \bmod 7$

$7 \overline{)40} \; (5$

35

$5 \overline{)35} \; (7$

35

0

$40 = 7(5) + 5$

$5 = 40(1) - 7(5)$

$M_2^{-1} = (1)$

$M_2^{-1} = 35^{-1} \bmod 8$.

$8\overline{)35}\,(4$
32
$3\overline{)32}\,(10$
30
$2\overline{)30}\,(15$
30
0

$35 = 8(4) + 3$.

$32 = 3(10) + 2$.

$2 = 32 - 3(10)$

$2 = 32 - [35 - 8(4)](10)$

$2 = 32 - 35(10) - 8(4)(10)$

$2 = 8(4) - 35(10) - 8(4)(10)$

$M_2^{-1} = 40^{-1} \bmod 7$:

$7\overline{)40}\,(5$
35
$5\overline{)7}\,(1$
5
$2\overline{)5}\,(2$
4
$1\overline{)2}\,(2$
2
0

$40 = 7(5) + 5$

$7 = 5(1) + 2$

$5 = 2(2) + 1$

$1 = 5 - 2(2)$

$1 = 5 - (7 - 5(1))(2)$

$= 5 - (7(2) - 5(2))$

$1 = 5 - 7(2) - (40 - 7(5))$

$1 = 5 - 7(2) - 40(2) + 7(5)(2)$

$= 5 - 7(5)(2) - 40(2)$

$= 5 - 7(5)(2) + 40(-2)$

$\bmod 7$

$7 - 2 = 5$

$M_2^{-1} = \cancel{8} \cdot 3$

$M_3^{-1} = 35^{-1} \bmod 8.$

$$
\begin{array}{r}
4 \\
8 \overline{)35} \\
\underline{32} \\
3 \overline{)8} \\
\underline{6} \\
2 \overline{)3} \\
\underline{2} \\
1 \overline{)2} \\
\underline{2} \\
0
\end{array}
$$

$35 = 8(4) + 3$

$8 = 3(2) + 2$

$3 = 2(1) + 1$

$3 - 2(1) = 1$

$1 = 3 - (8 - 3(2))(1)$

$= 3 - 8(1) + 3(2)$

$= 3(3) - 8(1)$

~~$3(2)$~~

$= (35 - 8(4))(3) - 8(1)$

$= 35(3) - 8(4)(3) - 8(1)$

$1 = 35(3) - 8(5)(3)$

$M_3^{-1} = 3$

(4) $x = [(3 \times 5 \times 1) + (1 \times 40 \times 5) + (6 \times 35 \times 3)] \bmod 280.$

$= [168 + 200 + 630] \bmod 280$

$\Rightarrow$ ~~998~~ mod 280.

$= \cancel{158}$ mod 280.

78

21/6/23.

1) $x \equiv 2 \bmod 7$

$x \equiv 3 \bmod 9$.

① $M = m_1 \times m_2 = 7 \times 9 = 63$

② $M_1 = \frac{63}{7} = 9$; $M_2 = \frac{63}{9} = 7$

③ $M_1^{-1} = 9^{-1} \bmod 7$

$7 \overline{)9(1}$

7

$2 \overline{)7(3}$

6

$1 \overline{)2(2}$

2

0

$9 = 7(1) + 2 \rightarrow 9 - 7(1) = 2$

$7 = 2(3) + 1$

$1 = 7 - 2(3)$

$1 = 7 - (9 - 7(1))(3)$

$= 7 - 9(3) - 7(3)$

$= 7 + 9(-3) + 7(-3)$

$7 - 3 = 4 \rightarrow M_1^{-1} = 4$

$M_2^{-1} = 7^{-1} \bmod 9$ ⟶ $7 = M_2^{-1}$

9) 7 (

④ $x = (a_1 z_1 M_1^{-1} + a_2 z_2 M_2^{-1}) \bmod M$

$= [(2 \times 9 \times 4) + (3 \times 7 \times 7)] \bmod M$

$= (72 + 147) \bmod M = (219) \bmod 63$.

$= 219 \bmod 63$.

$\equiv 30 \bmod 63$.

63) 219 (3

189

30

b.) $x \equiv 4 \bmod 5$

$x \equiv 6 \bmod 11$

1.) $M = m_1 \times m_2 = 5 \times 11 = 55$

2) $M_1 = \frac{55}{5} = 11$ $\qquad M_2 = \frac{55}{11} = 5$

3.) $M_1^{-1} = 11^{-1} \bmod 5$

5) 11 (2

10

1) 5 (5

5

0

$M_2^{-1} = 5^{-1} \bmod 11$

5) 5 (1 $\qquad$ 11) 5 (

5

0

$M_2^{-1} = 5$

$11 = 5(2) + 1$

$1 = 11 \cdot 5(2)$

$M_1^{-1} = 1$

4) $x = [(7 \times 11 \times 1) + (10 \times 5 \times 5)] \bmod 55$

$= (44 + 250) \bmod 55$

$= 294 \bmod 55$

$= 19 \bmod 55$

c) $x \equiv 7 \bmod 12$

$x \equiv 11 \bmod 12$

1) $M = 13 \times 12 = 156$

2) $M_1 = \frac{156}{13} = 12$

$M_2 = \frac{156}{12} = 13$

3) $M_1^{-1} = 12^{-1} \bmod 13$

$M_2^{-1} = 13^{-1} \bmod 12$

12) 12 (1
12
12) 12 (12
12
0

$12 = 12(1) + 1$

$1 = 13 - 12(1)$

$M_1^{-1} = 1$

13) 12

$M_1^{-1} = 12$

13) 12 (1
12
1) 12 (12
12
0

$13 = 12(1) + 1$

$1 = 13 - 12(1)$

$M_2^{-1} = (1)$

4) $x = (7 \times 12 \times 12) + (11 \times 13 \times 1) \bmod 156$.

$= (1008 + 143) \bmod 156$.

$= 59 \bmod 156$.

26/8/23.

Miller Rabin Test:

① $n-1 = m \times 2^k$

② $T \leftarrow a^m \bmod n$.

for iteration ② $T \leftarrow T^2 \bmod n$.

$(k-1)$ iterate times.

finally $\begin{cases} +1 \longrightarrow \text{composite no.} \\ -1 \longrightarrow \text{prime no. (1 extra)} \end{cases}$

CRT

Quadratic congruence:

$x^2 \equiv a \pmod n$

$a_2 x^2 + a_1 x + a_0 \equiv 0 \pmod n$

$a_2 \to 1$, $a_1 \to 0$

$x^2 + a \equiv 0 \pmod n$

Quadratic residues → soln exists

Quadratic non residues → no soln exists.

Q) $\begin{cases} x^2 \equiv 8 \pmod{23} \\ x^2 \equiv 2 \pmod{11} \\ x^2 \equiv 7 \pmod{19} \end{cases}$

D $x^2 = 3 \pmod{23}$ → 0 to 22.

$0^2 \bmod 23 = 0$

$1^2 \bmod 23 = 1$

$2^2 \bmod 23 = 4$

$3^2 \bmod 23 = 9$.

$4^2 \bmod 23 = 16$

$5^2 \bmod 23 = 2$

$6^2 \bmod 23 = 36 \bmod 23 = 13$

$8^2 \bmod 23 = 64 \bmod 23 = 18$

$9^2 \bmod 23 = 81 \bmod 23 = 12$

$10^2 \bmod 23 = 8$

$11^2 \bmod 23 = 18$

$12^2 \bmod 23 = 6$

$13^2 \bmod 23 = 8$

$14^2 \bmod 23 = 20$

$15^2 \bmod 23 = 18$

$16^2 \bmod 23 = 3$

$17^2 \bmod 23 = 13$

$18^2 \bmod 23 = 2$

$19^2 \bmod 23 = 16$

$20^2 \bmod 23 = 9$

$21^2 \bmod 23 = 4$

$22^2 \bmod 23 = 1$

Quadratic Residues:

0, 1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18, 20.

Non Quadratic Residues

5, 7, 10, 11, 14, 15, 17, 19, 21, 22.

② $x^2 \equiv ? \pmod{11}$ ⟶ 0 to 10.

$0^2 \bmod 11 = 0$

$1^2 \bmod 11 = 1$

$2^2 \bmod 11 = 4$

$3^2 \bmod 11 = 9$

$4^2 \bmod 11 = 5$

$5^2 \bmod 11 = 3$

$6^2 \bmod 11 = 3$

$7^2 \bmod 11 = 5$

$8^2 \bmod 11 = 9$

$9^2 \bmod 11 = 4$

$10^2 \bmod 11 = 1$

Quadratic

0, 1, 3, 4, 5, 9.

NQR

2, 6, 7, 8, 10.

② $x^2 \equiv 7 \pmod{19}$

$0^2 \bmod 19 = 0$

$1^2 \bmod 19 = 1$

$2^2 \bmod 19 = 4$

$3^2 \bmod 19 = 9$

$4^2 \bmod 19 = 16$

$5^2 \bmod 19 = 6$

$6^2 \bmod 19 = 17$

$7^2 \bmod 19 = 11$

$8^2 \bmod 19 = 7$

$9^2 \bmod 19 = 5$

$10^2 \bmod 19 = 5$

$11^2 \bmod 19 = 7$

$12^2 \bmod 19 = 11$

$13^2 \bmod 19 = 17$

$14^2 \bmod 19 = 6$

$15^2 \bmod 19 = 16$.

$16^2 \bmod 19 = 9$

$17^2 \bmod 19 = 4$

$18^2 \bmod 19 = 1$

QR:

0, 1, 4, 5, 6, 7, 9, 11, 16, 17,

NQR:

2, 3, 8, 10, 12, 13, 14, 15, 18.