Computer Security means protecting Computer's data from harm, theft or unauthorized access and also preserve Integrity, availability and Confidentiality of Info system.

Core of Computer Security /concepts

- Confidentiality, Integrity, availability.

Confidentiality: It means keeping data secured and not allowing unauthorized access.

Cover 2 concept

Data confidentiality: only authorized people or system can see or Read private or confidential info.

Privacy: Locking personal information., Individuals only acess which is related to him. only he can read it & edit and store

Example: GeMail Acc is protected by a password. Only you can read yr email

techniques used: Encryption, biometric login, Access Control. Lists.

Integrity: Data should be Correct, Complete and not changed by anyone without permission.

data Integrity: data is not modified during transfer & storage: small change can occur big travel.

System Integrity: free from inadvertent unauthorized manipulation of the system.

Ex: send someone file over a Network but someone change it during transfer for Integrity Lost

Techniques used: Hash function, checksum, Digital Signatures.

Availability: Data and system should always be available when needed.

. user should acess anytime anywhere

. This protects against crashes or attack that block access.

Techniques used: Backups, Redundant system. Protect from (DoS), attack)

Eg → If hospital Server down doc, can't acess patient records.

Two other Security Concepts are

Authenticity: Make sure that user or data is real and trusted. [Login with fingerprint]

Accountability: tracking who did and what and when in System.

System Logs show the user actions.

Challenges of CS:

Cyber attack: hackers try to break into system. (Phishing, Dos attack) They need only one weakness for attacks hack

Weak password: It can be gained one hand.

Insider threats: Attenders from people inside the organization.

Cloud computing: Storing data online needs strong protection.

Balancing security: To much security can make system hard to use

Changing tech: New threats comes with new tech

Designer challenge: designer must find and fix all weakness for secure

Security as an afterthought: Security must planned from design & development time not, after mares.

OSI Security Architecture

Security attack, Security Service, Security Mechanisms.

Passive Security Attack: To secretly observe or listen. data being transmitted.

types
- Release of Msg contents.
  - reading email, calls, files without permission.
- traffic analysis
  - Even if msg is encrypted, attackers can watch patterns (who talk, to whom, when and How)

Active attack: To change, fake, block data being sent.

Masquerade attack: hackers login as someone else.

Replay attack: Captures valid data transmission and retransmits them to deceive the system.

e.g. Interrupt bank transaction and resending it to duplicate transfer.

Modification of Msg: Changing the recipients acc Num in fund transfer Req.

Denial of Service (DoS): Makes system slow unavailable

Eg- flooding a server with fake request

Security Services (what we want)

→ It is a Communication Service that provided by a system to give a specific kind of protection to the system resources. It ensure Secure Communication across network

Authentication:

- Verify the identity of users or systems.

Eg login with pass & id. and also OTP.

Access Control: It control who can have access to a resource. Grants and denies permission to one System Resource

Ex → student can't acces teacher data.

Data confidentiality: protection data from unauthorized users. (Use Encryption (AES, RSA))

Ex → whatsup use end to end encryption to protect chats & calls.

Data Integrity: Data should be correct or not changed data can be received are exactly as send by entity. (use Checksum, hasing).

Ex → Send file content not be changed.

Non Repudiation: Someone can't deny they performed the action

Ex - Send email with digital signature your can't say i dont sign it.

Intrusion Detection System (IDS): Detect suspicious activities

Ex → Alert admin if unusual login

Security Mechanisms

Specific Security Mechanism:

Encipherment (Encryption) ← use algorithm
- Converted data into secret code (Whatsapp encrypted end to end end)

Digital Signature: Confirm identity of the sender ensure msg not changed.

Eg → a signed Email confirm identity

Access Control: Access only Authorized user

Eg → Stu can't access teacher dashboard

Data Integrity: Ensure data should be correct and not changed

Eg → download file hash clk use to clk if it altered

Pervasive Security Mechinum: (prumd Everywhere)
help other

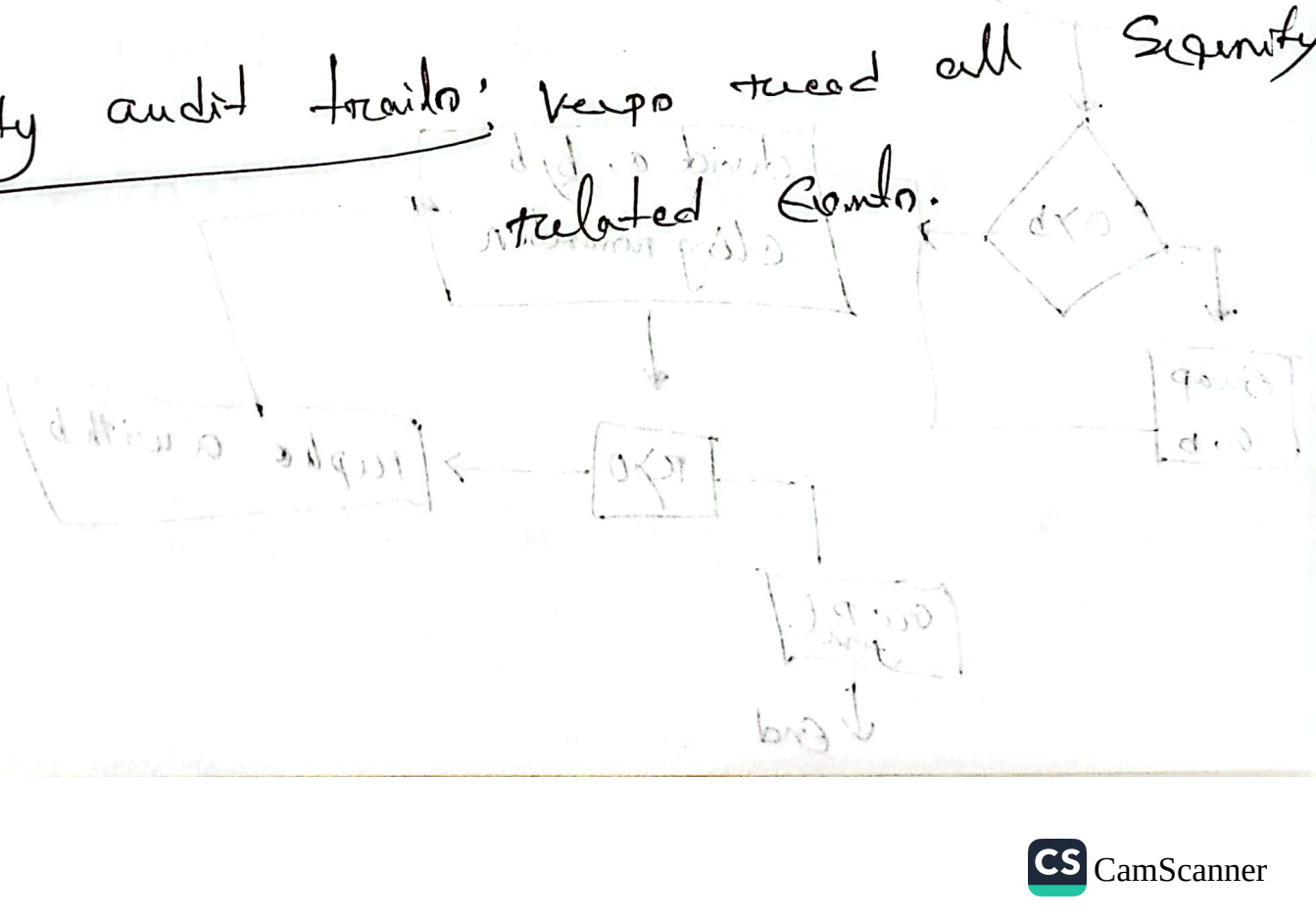
Security recovery: Ensure system can recover from unexpected
Eg → Backup data so that it can recover if
delete by hacker.

Trusted functility: ensure system behaves as expected.

Security Labels: Tag that define security level of
data.

Event detection: Identify security related event.
(intrusion attempts)

Security audit trails: keeps record all security
related events.

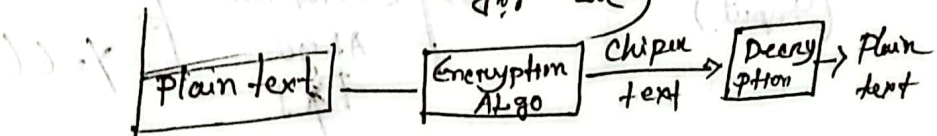


Segment 2

Cryptography is a technique of securing information through the use of codes to secure format. To ensure that only the intended person can read & understand the data.

plain text → Normal massage

Cipher text → transformed massage (understand only key true)



Feature of Cryptography

→ Confidentiality, Integrity, Authentication, Adaptibility

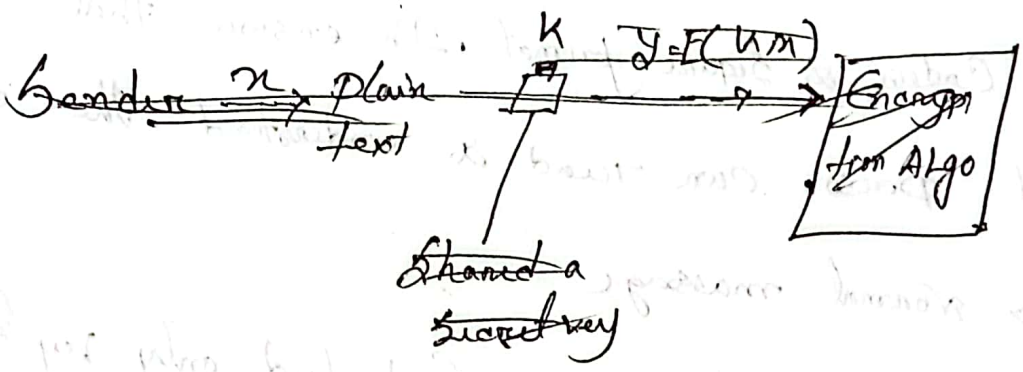
Symmetric key cryptography / conventional

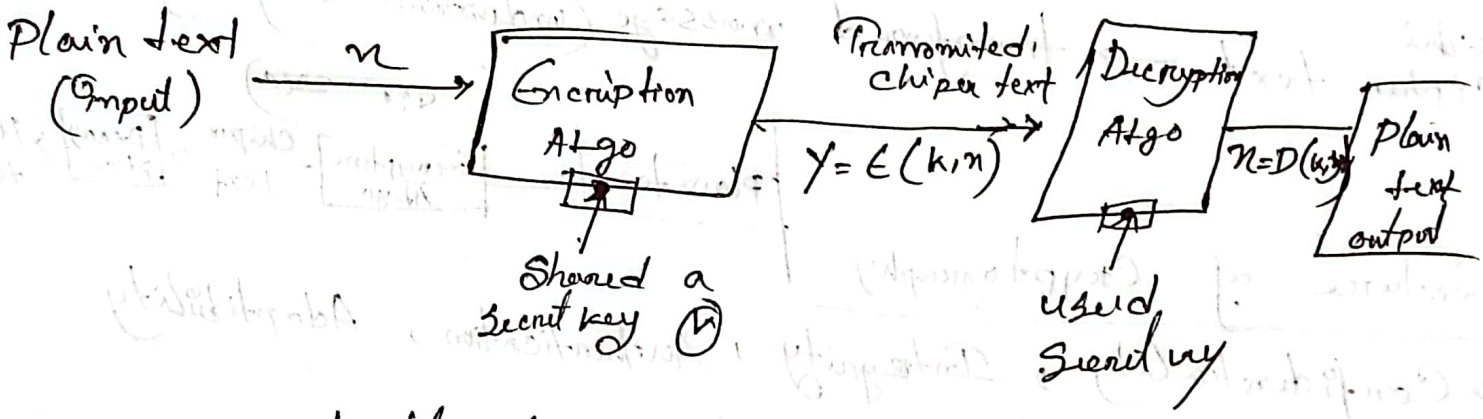
5 thing need

Secret key: used encryption and decryption. Exact substitutions and transformation performed by algorithm depend on the key.

plain text: This is orginal intelligible msg or data that used as algorithm input.

Encryption Algorithm : It perform various substitution and transformations on plain text.



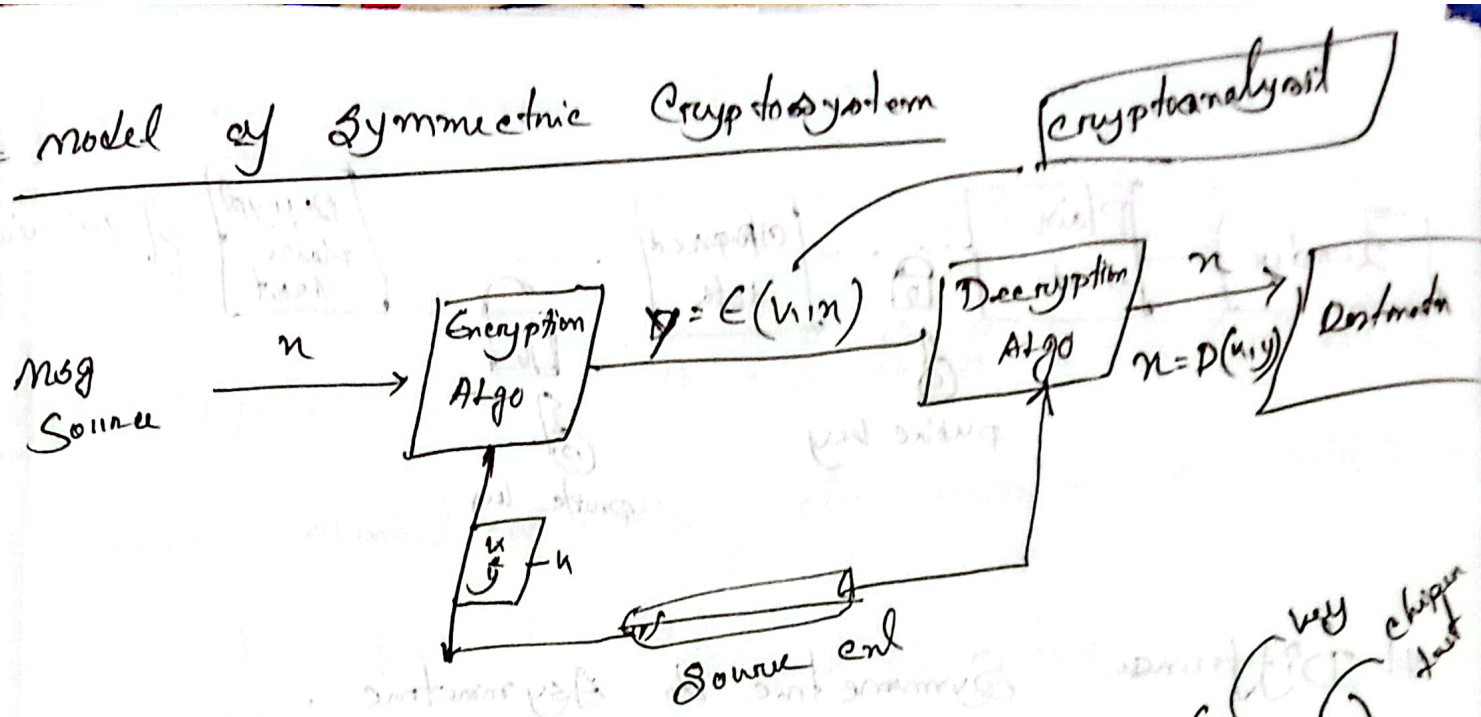


Model of Symmetric encryption

Chiper text : It depends on plain text and the secret key. It is the coded message (unintelligible)

Decryption Algorithm : Mainly it is a reverse encryption algorithm. It takes chiper & key and produce original Plaintext

model of symmetric cryptosystem



here $y = E(k, x)$ — plain text, key, Encryption Algo, chiper text

$x = D(k, y)$ — key, chiper text, plain text, Dycription Algo

Asymmetric key Cryptography : public key

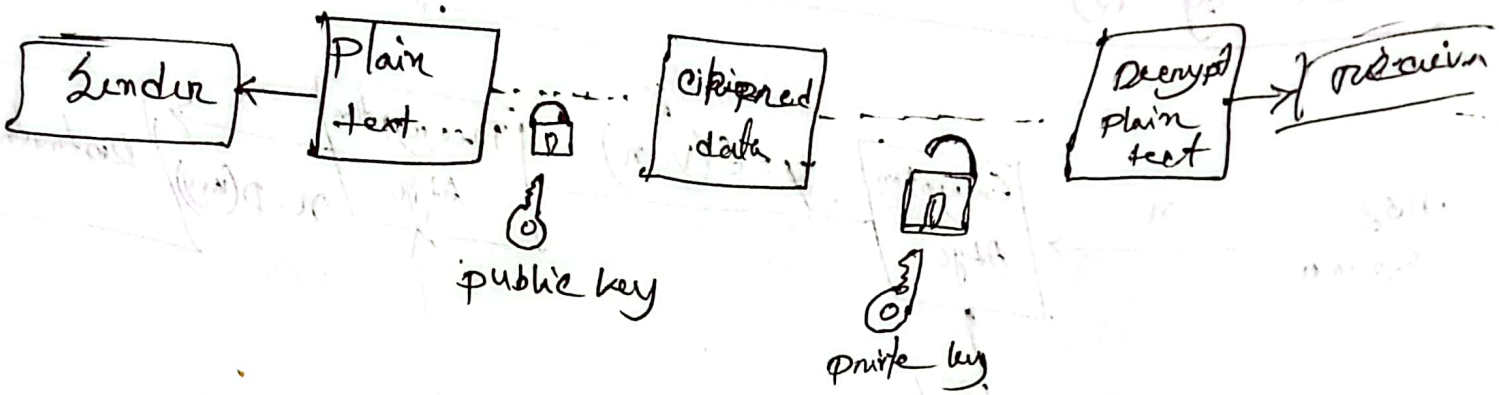
It is a type of encryption where 2 key used.

public - shared who with anyone

private - kept Secret the owner

Works . Sender encrypts the msg using Reciver public key

- only reciver private key can decrypt the msg.



Difference Symmetric & Asymmetric.

Symmetric	Asymmetric
• One key same for encryption & Decryption	• Two keys (public & private)
• key must share secretly	• No need share private key
• faster & Efficient	• Secure resource heavy.
• if key leaked all exposed	• More secure for communication.
• AES, DES, Blowfish	• RSA, ECC, DSA
• Wifi, file encryption, Bluetooth, (Secret key used encrypt and decrypt	• Secure email, Secure website Online banking, → pass from your bank (user transaction bank to (user

private key

One time pad (Vernam chiper)

a	b	c	D	E	f	g	h	I	J	k	L	m
0	1	2	3	4	5	6	7	8	9	10	11	12

n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

plain text : HELLO

key : XMCKL.

1st convert Alpabet as the value number st with (0-25)

H	E	L	L	O	← plain tex
7	4	11	11	14.	

X	M	C	K	L	← key
23	12	2	10	11	

chiper = (key + plain text) mod 26.

26 বড় হলে যোগ করে just (৩০ - 26) করলে mode done

30	16	13	21	25	(Add)
4	16	13	21	25	(Mod)
E	Q	N	V	Z.	(Encrypted)

Decryption

key X M C K L
23 12 2 10 11

E Q N V Z
4 16 13 21 25 (chipen)

~~chipen~~ =
plantext = (Chipen − key + 26) mod 26

	4	16	13	21	25
(−key)	−23	−12	−2	−10	−11
	−19	4	11	11	14
(+26)	7	4	11	11	14
	↓ H	E	L	L	O

— key ⊖ হলে ⊖ হলে +26

26+
যখন ⊖ হবে

Decrypted msg − HELLO

Cryptanalysis

It is a process of trying to break a cipher (find orginal msg or key) without knowing the key.

Attackers use structure of algorithm, clues about msg and try to guess orginal message (plaintext) and find key for decrypt the unreadable cypertext

Brute force attack:

- Attackers try every possible way find the key one by one when correct key found, the msg turns into something readable. almost half of the key tries for find right one

Encryption Square of It

- Cost of break cyper exceeds the value of encrypt info.
- The time required to break the cipher exceeds the lifetime of the info. (donven mes hoi gle সেকেন্ড কুড়ি)

~~Substitution~~

Substitution Ciper. (Caesar)

here letter of plaintext are Replaced by other letters or by number or Saymbol

একবার repled হলে 2nd time use হবে না

Encryption

$c = (P+3) \bmod 26$

Plain	A	B	C	D	E	Z
Ciper	D	E	F	g	h	c

key shift 3

→ mod করে

(plain + key) mod 26

Decruption

(ciper − 3) mod 26

	D	E	F	g	h	c
−3	3	4	5	6	7	2
	A	B	C	D	E	Z

3 − 2 = −1 mod 26 = 25 — Z

[26 + −1 = 25]

Transposition techniques

Change the plain text position so called transposition.

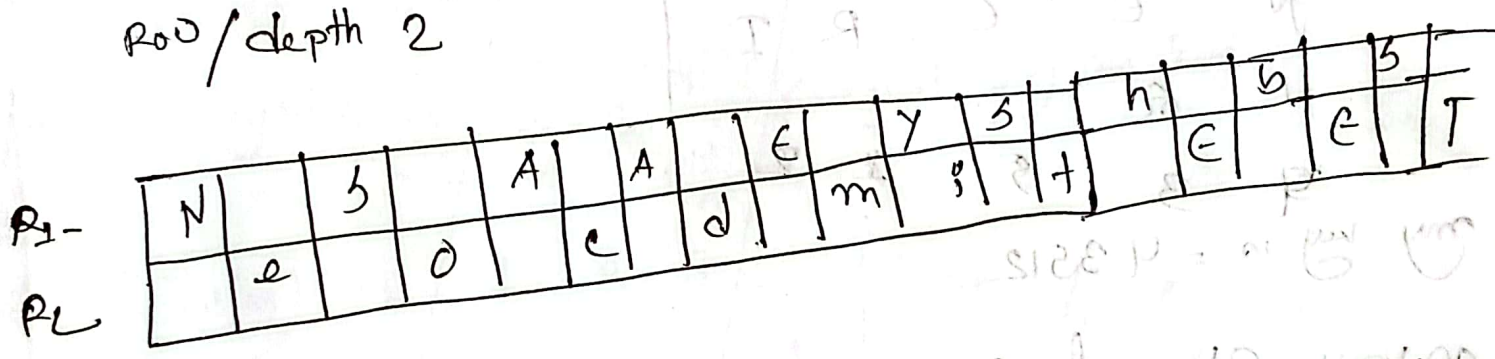
2 way (key less) fail fence (simple) ——— row

Column Transposition.

Row wise

Plain text = Neso Academy is the best

Row / depth 2



Chiper text: NsAAeysh,bsh bs, eocdmistEET

P1 P2

Colmun Transportion

Plain text : Five Minutes EngINEERing

key = 43512 [Clm এর ওপর গুরু] 5.2r key

Clm →

4	3	5	1	2
F	I	V	E	M
I	N	U	T	E
S	E	N	G	I
N	E	E	R	I
N	G			
4	3	5	1	2

key এর ওপর Clm বানালো

my key is = 43512

as key Clm put on

Chiper text = ~~ETGR~~ ~~VUNE~~ ~~MEII~~ ~~FISNN~~ (4, 3, 5, 1)

~~INEEG~~ (2)

ETGR MEIT INEEG FISNN

VUNE.

(4) Stream Cipher

Stream Cipher	Block Cipher
• here Length define bits & bytes	here block size 64 or 128 bits
• Design is so coplex	• design is so simple.
• Principle is Confusion	• principle is Confusion & Diffusion.
• Speed is foten	• Speed is slower
• Encryption done by CFB, OFB	• Encryption done by ECB & CBC
• Decryption done by XOR	• reverse of Encryption
• Vernam cipher (Example)	• DES, AES (Example)

Bigram frequency

A bigram is a sequence of 2 consecutive words from given text.

bigram frequency refers to how times each pair of words (bigram) appears in the text.

2 টা pices থাকে

I Love Coding. I Love mango.

→ I Love — 2 time
Love Coding — 1 time
Love mango — 1 "

frequency যখন same জিনিস দুইবার থাকবে তখন লিখে 2 times হবে

Trigram frequency:

Sequence of 3 consecutive words from a given text.

Trigram frequency refers that how times each 3 word sequence appears.

Ex → I Love Coding, I Love Coding on Python

I, Love, Coding. — 2 times

Love Coding on — 1 time

Coding on Python — 1 time.

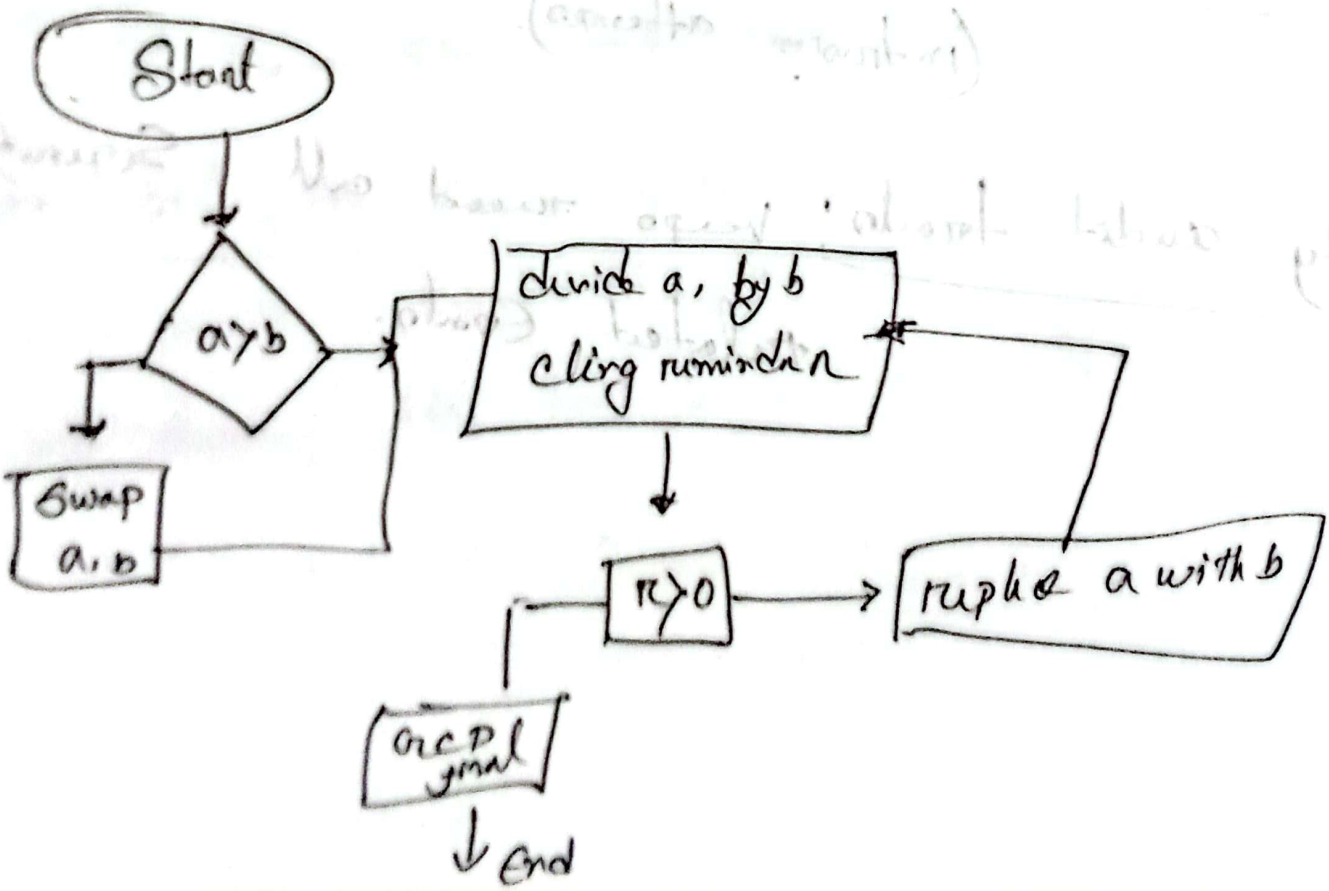
Fig 3.

Euclidean Algorithm: Determining the GCD of 2 positive integer.

Two integer are relatively prime (Co prime) if there is common diveson GCD is 1.

if GCD greater than 1 not Co prime.

Euclidan Algorithm to find GCD.



* find GCD of (450, 120) ? find 2 number are co prime.

450, 100
a b

a > b

450 > 120 (yes)

Next devide a/b (calleing remindin)

450 / 120 = 3 and reminder 90.

450 = 3 × 120 + 90

120/90 = 1 reminder 30

→ 120 = 1×90 + 30

90/30 = 3 reminder 0

→ 90 = 30×3 + 0 — here GCD find

GCD in 30

here GCD = (450, 120) = 30 not 1 [Not co prime]

AES

[Advanced Encryption Standard]? Symmetric block cipher

AES use to encrypt data (like passwords, files or msg) so that only authorized people can read it.

AES works Step by Step

Plaintext (Input)

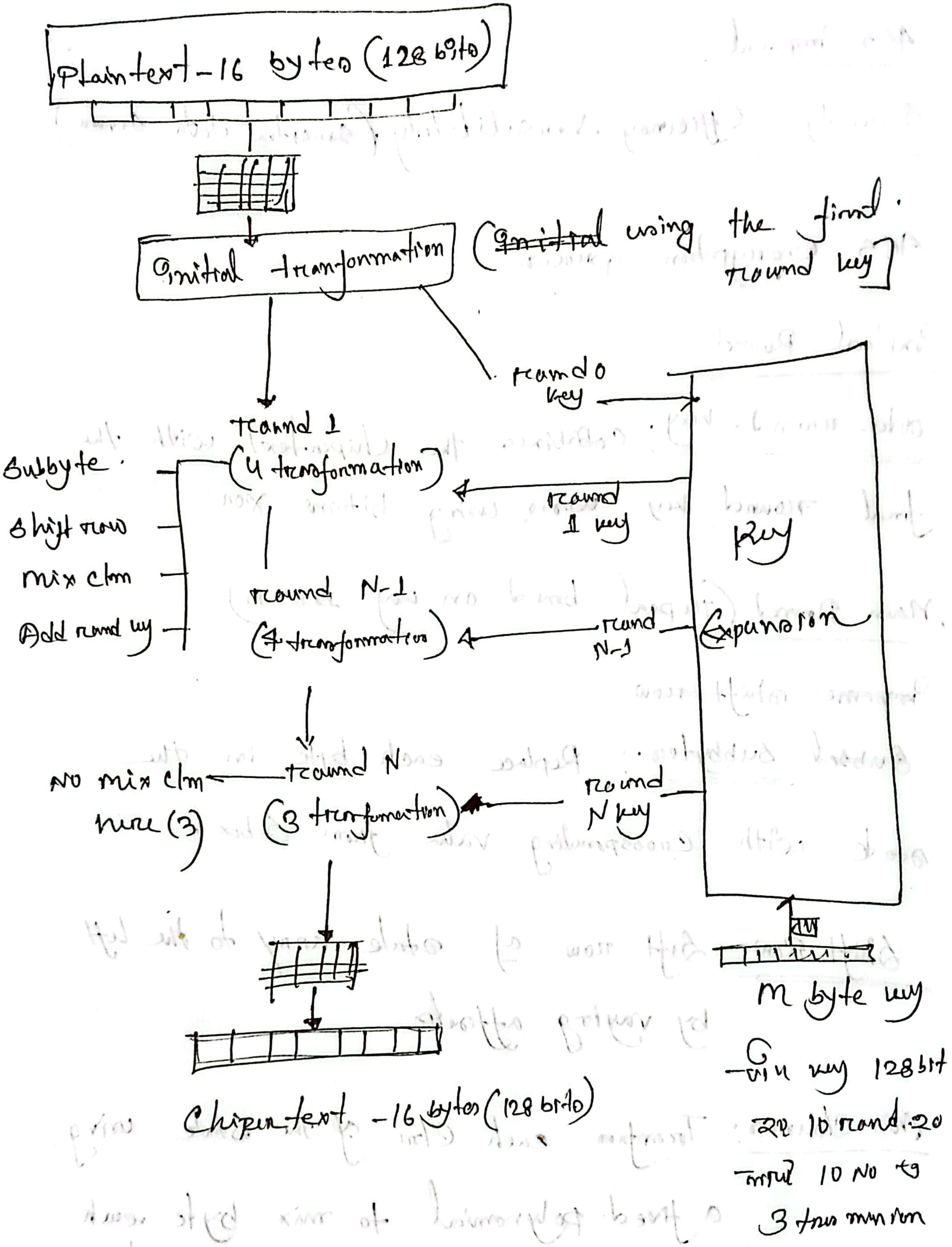
- orginal data we want to protect.
  Size 16 bytes = 128 bits.

Key (Encrypt the plaintext)

128 bits = 10 rounds, 192 bits = 12 rounds.
256 bits = 14 rounds.

Key Expansion:

Key is Expanded into multiple round keys.
- one key is used for round of transformation.


Plaintext - 16 bytes (128 bits)
Initial tranformation
(~~Initial~~ using the first round key)
round 0 key
round 1
(4 tranformation)
Subbyte
Shift row
mix clm
Add round key
round 1 key
Key
Expansion
round N-1
(4 tranformation)
round N-1
No mix clm
here (3)
round N
(3 tranformation)
round N key
M byte key
key 128 bit
10 round
10 No
Chipen text - 16 bytes (128 bits)

AES Important.

Security, Efficiency, Versatility (Sensitive data secure)

AES Encryption process.

Initial Round

add_round_key: combines the chipertext with the final round key using bitwise xor

Main Round (repeat based on key 128=10)

~~Inverse shift row~~

~~Subset~~ subbytes: Replace each byte in the state with corresponding value from S box.

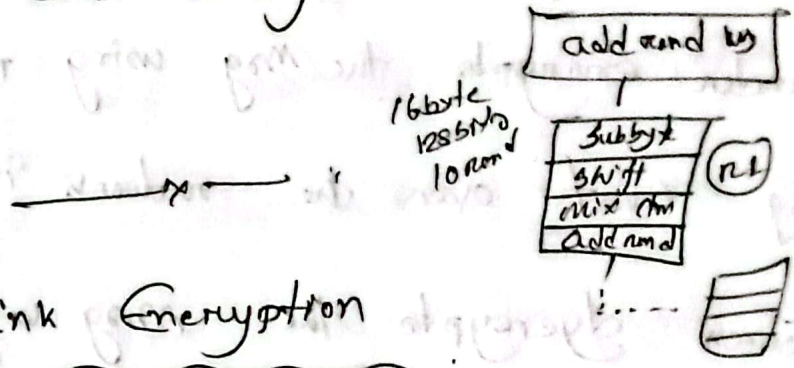
Shift Row: Shift row of state array to the left by varying offsets.

Mix Columns: Transform each c/m of the state using a fixed polynomial to mix byte each c/m.

add round key again.

Final Round : Repeats subbyte, ShiftRow, and AddroundKey step but omit the MixColumn transformation.

AES Decryption : To retrive original data, AES perform the inverse of each encryption step in reverse order using same key



Link Encryption

Link encryption secures data by encrypting and decrypting info at every node or network switch. It passes through Router just at end point. It ensure all data header & routing info protect.

Disadv : In every switch msg decrypt is mendatory. For know the address from header. So msg can be vulnarable.

use unique key

End to End Encryption

here [redacted] and receiver only communicate by private key. It guarantees that only the intended sender and receiver can access and understand data the data pass through many way.

- Sender encrypts the msg using receiver public key
- Msg sent over the network in encrypted form.
- receiver decrypts the msg using their private key

Adv - router switch can't see data
- protect data from unauthorized individuals.

Using Both Link & E2E :

- E2E keeps of user data safe from at to end
- Link encryption secures the entire packet during transmission across each network segment.

Key distribution

It is the process of sharing secret encryption keys securely between parties who want to communicate.

Distributed A → B many ways

* A can select a key physically deliver it.
* third party select key and physically deliver A & B
* If A & B previously & recently used a key, one party transmit the new key to other encrypt using old one
* If A & B has encrypt connection third party C can deliver a key on encrypted links to A, B

Key Distribution Center (KDC)

It used for key sharing easy and safe way

2 level key used

Master key: Each user share a secret key with KDC permanent same

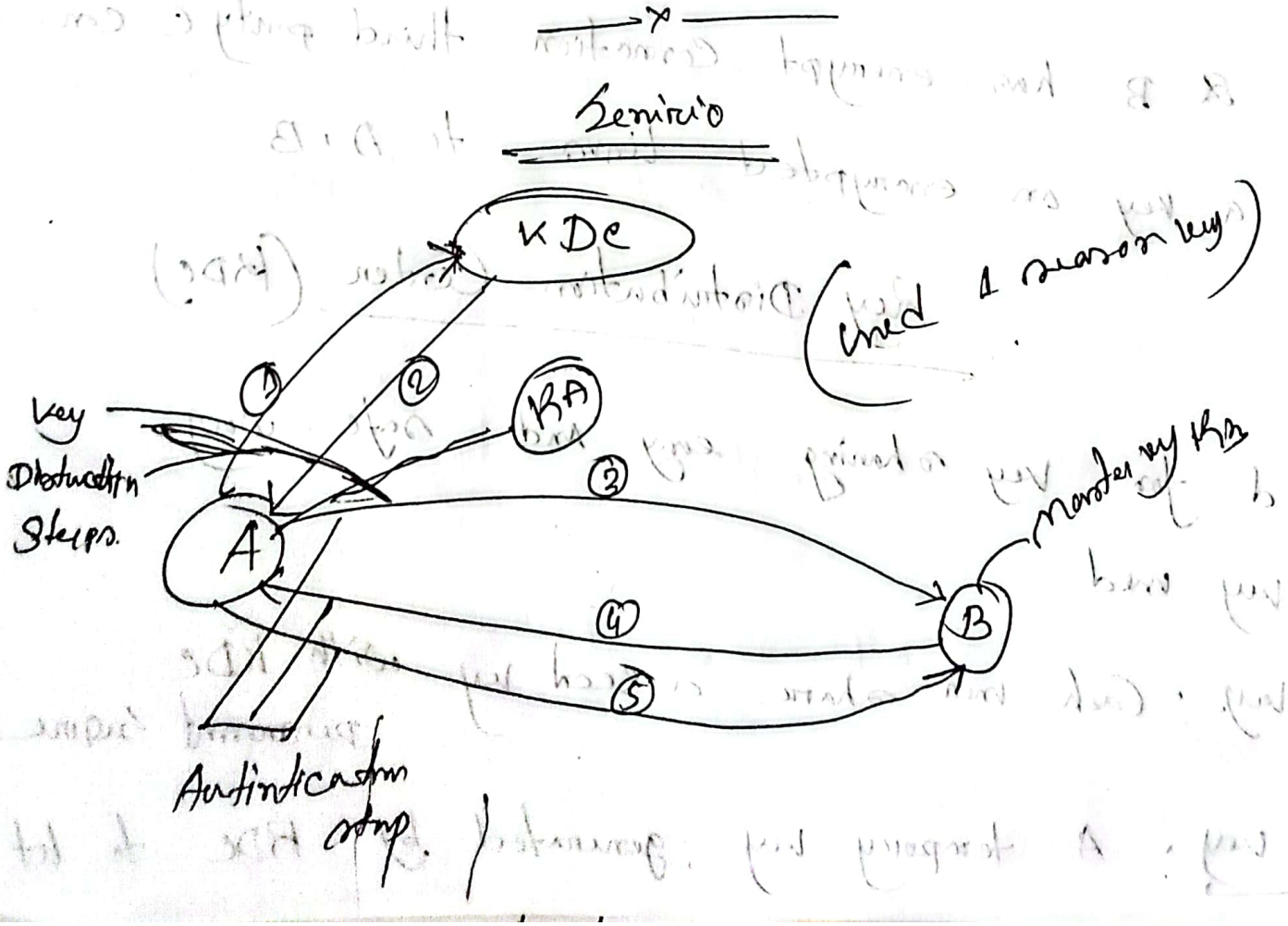
Session key: A temporary key generated by KDC to let

User Communicate Securely, used for one Session and then discarded.

- Session key ~~distribution~~ transmitted in encrypted from using a master key that is shared by the key distribution center (KDC)

of N entities communicate as many way $\frac{N(N-1)}{2}$ Session key used at once. N master required.

(Frequently Session key change ~~req~~ req)



A user A want to send msg B securly

Step using KDC (3rd party)

① A sends a req to KDC for a session key talk B.

② ~~The KDC~~ A also send nonce (random number) to keep the request unique (N_1) (or timestamp)

③ The KDC creates a session key (K_s) and prepare reply (both send to A)

- one part for A ⇒ include a Sesn key and original request(N_1) encrypted with (K_A) master key (A corresponding key)

- another for B ⇒ Which includes Sesn key and A's ID (IDA) with B's master key (K_B) [K_s [K_s] ID_A)

④ A recv the reply decrypts its part using (K_A) to get Sesn key (K_s).
and sends B's part to B (because he can't open it bez of B's master key)

(5) B decrypts it using (K_b) and get same Session Key also known signal from A.

Now both A & B securely talk each other