Information security - I (i)

Cryptographic Algorithms (and) protocols can be grouped into 4 main areas

Symmetric encryption

- used to conceal contents of the blocks or streams of data of any size, including messages, files, encryption keys & Passwords

Assymetric encryption

- used to conceal Small blocks of data such as encryption keys, hash values. which are used in the digital Signatures

Data Integrity Algorithms

- used to protect blocks of data, Such as messages from alterations

SADA

Authentication Protocols

- schemes Based on the used the cryptographic Algorithms designed to authenticate the identity of entities.

Network or Internet security consist of

measures to deter, Prevent, detect, and correct security violations. that involve the Transmission of Information

what is computer security?

According to NIST Computer society handbook

the Protection afforded to an automated information system in order to attain the applicable objectives of preserving the Integrity, availability, confidentiality of Information system resources

computer security objectives !.

Confidentiality

data confidentiality

ensures.. not disclosed to unauthorized

Privacy

each can control information only they should be capable of accessing

↑ ensuring this

Integrity

Data Integrity

ensuring programs or data is changed only in Authorized manner

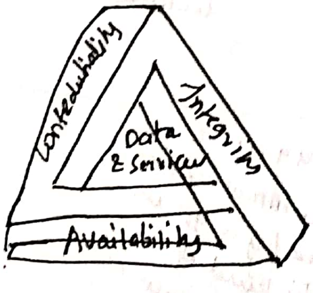
System Integrity

ensuring... System is unathorizedly manipulated

Availability

Assures system works promptly and not denied to authorized users

The CIA Traid



Additional concepts

Authenticity

- verifying users and their data are from a trusted source or not

Accountability

- The security goal that generates the requirement for actions of an entity to be traced as to hold it accountable.

Breach of security
Levels of Impact

High	• The loss could be severe or Catastrophic effect on everything
moderate	• This would have a serious effect on organization, individuals.
Low	• This loss could be expated to have a limited damage

OSI Security Architechture

- Security Attack
  → Any Action that Comprises the Security of Information owned by an organization.
- Security mechanism
  → A process that is designed to detect, prevent or recover from a Security attack.
- Security service
  → A processing or communication Service that enhances the security of the data processing systems and information transfers of an Organization.
  → Intended to counter security attacks, and they make use of one or more security mechanisms to provide the service

Computer security challenges

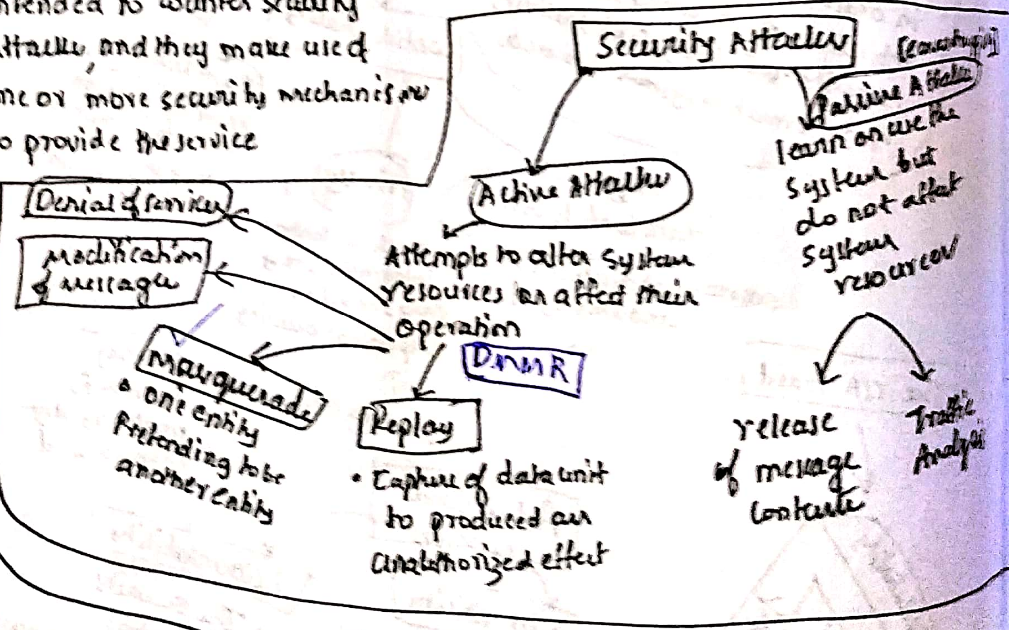
- security not simple
- potential attacks on the security features must be considered
- Requires constant monitoring
- There is always an tradeoff between efficiency and user friendly operation
- security mechanisms typically involve more than a particular Algorithm or protocol.

Threat

A potential for violation of security, a capability that can cause harm.
A threat is a possible danger that might exploit a vulnerability

Attack

An Assault on system security that derives from an intelligent threat & violate the security policy of a system


Security Attacks
[eavesdropping]
Passive Attacks
learn or use the system but do not affect system resources
release of message contents
Traffic Analysis
Active Attacks
Attempts to alter system resources or affect their operation
DMMR
Denial of service
modification of message
Masquerade
• one entity Pretending to be another entity
Replay
• Capture of data unit to produced an unauthorized effect

Security services

Defined By X.800 as

A service is a protocol layer of communicating open Systems and ensures adequate security of systems

Defined by RFC 4949 as

: A processing or communication service provided by a system to give specific kind of Protection to System resources

X.800 security services → Non Repudation → Prevention of Dos

DADAN

Authentication

concerns whether the source of user & its data is Authentic or not

- Peer entity authentication
- Data origin authentication

Access Control

limiting & controling the access to host system & preventing unauthorized usage of system [Access rights]

Data confidentiality

Protection of data from unauthorized disclosure

- Connection confidentiality: Protect all data of user on a connection
- Connectionless confidentiality: Protection of all data in single user block
- Selective field confidentiality: confidentiality of all selected fields in single data block
- Traffic flow confidentiality: Prevention of information disclosure obtained by observing network

CCST

Data Integrity

Assurance that data is exactly received as sent by the sender

- connection Integrity with Recovery
- connection Integrity without recovery
- connectionless Integrity
- Selective-field connection Integrity
- selective-field connectionless Integrity

Security mechanisms

Specific security mechanisms

- encipherment
- Digital signature
- Access controls
- Data Integrity
- Authentication exchange
- Traffic Padding
- Routing control
- Notarization [3rd party]

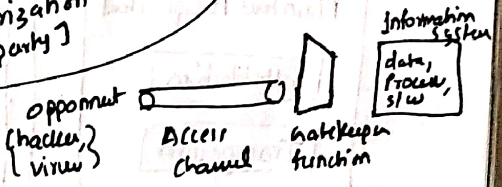
EDAD TRN

Pervasive security Mechanisms

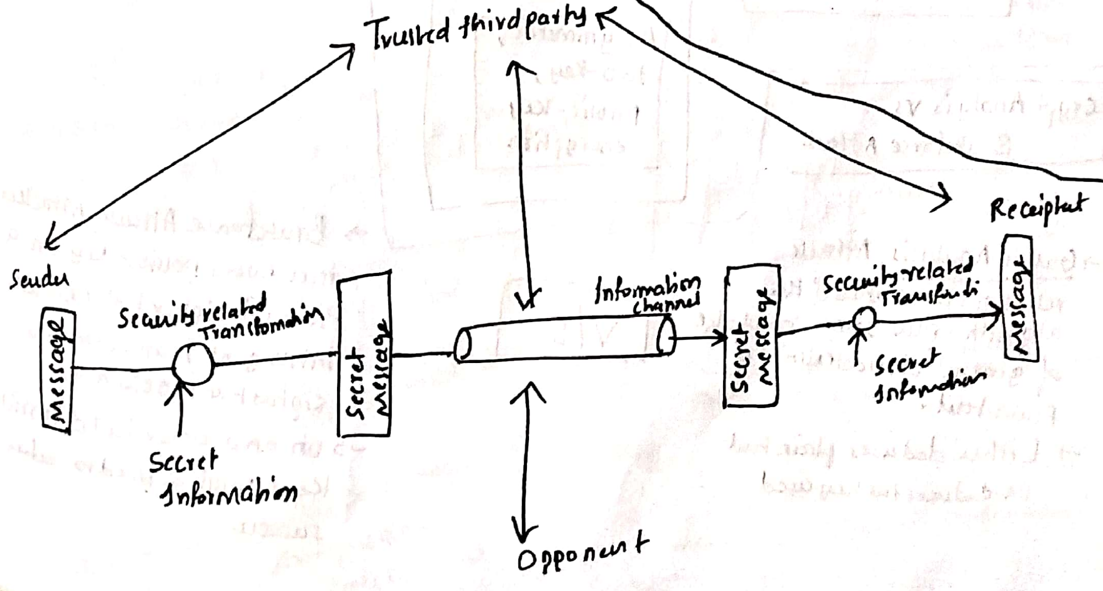
- Trusted functionality
- security labels
- event detection
- security audit traile
- security recovery

SESTS

Network Access Security Model



Model for Network security



Informationsecurity – I(ii)

Symmetric Encryption

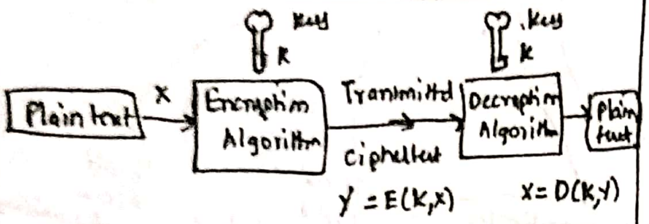
conventional / single-key encryption

was only type encryption in 1970's

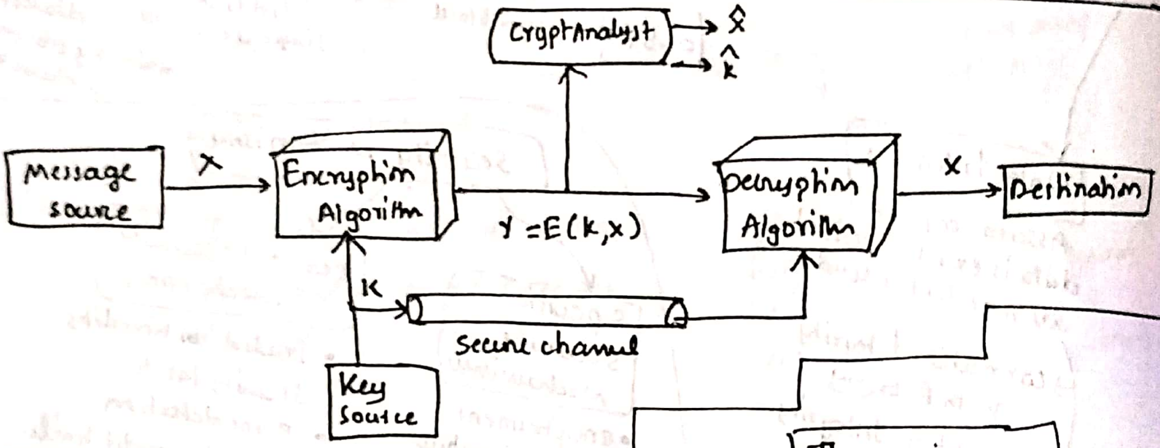
Basic Terminology

- Plaintext
- ciphertext
- encipherment / encrypting
- Deciphering / decryption
- Cryptography
  - study of cryptography encryption
- cryptographic system / cipher
  - schemes used for encryption
- Crypto Analysis
  - Techniques used for deciphering a message without any knowledge of the enciphering details
- Cryptology
  - Areas of Cryptography and Crypto Analysis together

Model of symmetric encryption



model of symmetric Cryptosystem



Cryptographic systems

- Categorized into three dimension

Types of methods used for Transforming Plaintext to ciphertext
- Substitution
- Transposition

The number of keys
- Symmetric, single-key, conventional encryption
- Assymmetric, two-key, Public-key encryption

The way in which plaintext is processed
- Block cipher
- Stream cipher

Crypt Analysis vs Bruteforce Attack

→ Crypto Analysis, Attack relies on the nature of the algorithm plus some knowledge of general charecteristics of plain text.

→ Either deduces plaintext or deduces the Key used

V/S

→ Bruteforce Attack, Attacker tries every possible key on a Piece of cipher text until an intelligent translation into ciphertext is obtained

→ On an average half of Possible Keys must be tried to achieve success

Types of Attacks on encrypted messages

Type of Attack	Known to Crypt Analyst
cipher text only	• encryption algorithm • ciphertext
Known plaintext	• encryption Algorithm • ciphertext • one or more plaintext - ciphertext ciphers formed with secret key
chosen plaintext	• encryption Algorithm • ciphertext ① → • Plaintext message choosen by cryptanalyst, together with its corresponding cipher text generated with secret key
chosen ciphertext	• encryption algorithm • ciphertext ② → • ciphertext chosen by crypt analyst, together with its corresponding decrypted plaintext generated with secret key
choosen text	• encryption algorithm • cipher text • ① • ②

Encryption scheme security

unconditionally secure → no matter how much time the opponent has it should be impossible for them to decrypt

computationally secure → The cost of breaking cipher exceeds the value of encrypted information

Substitution technique

In which one of letters are replaced by other letter symbols or numbers

If plain text is viewed as a sequence of bits, then substitution involves replacing plain text bit patterns with cipher text bit patterns.

Caeser cipher – julius cipher

simplest & earliest known

a b c d e f g h i j k l m n o p q r s t u v w x y z
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
(or) a = 0 , z = 25

Encryption

$$C = E(K, P) = (P+K) \bmod 26$$

Decryption

$$P = D(K, C) = (C-K) \bmod 26$$

But you can perform the Brute force Analysis of the Caeser cipher [illegible] key to decipher

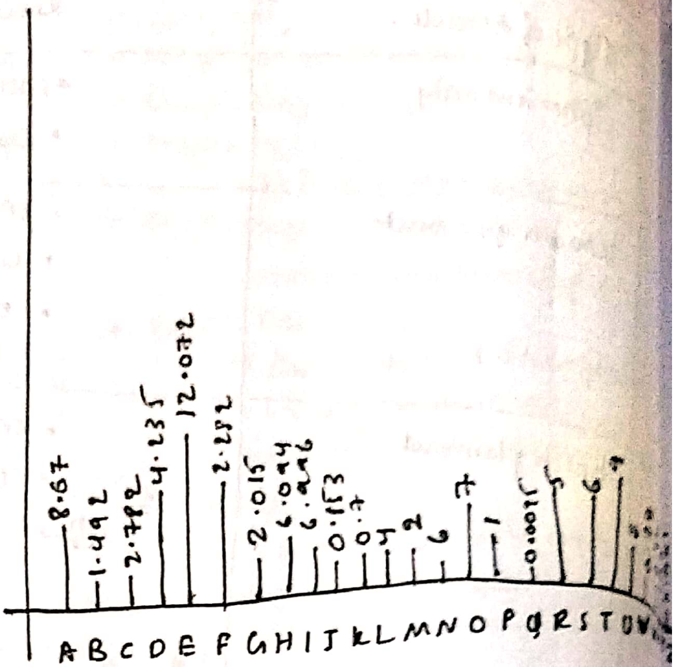
PHHW PH OIWHU

Key
1 – – – –
2 – – – – –
3 meet me after ✓ → deciphered
25

Monoalphabetic cipher

- permutation
  - → of a finite set of elements
  - 'S' is an ordered sequence of all elements appearing exactly once.
- → If the cipher line can be any permutation of 26 alphabetic charecters then there are 26! or greater than 4 x 10^{26} possible keys
  - "This is 10 orders of magnitude greater than key space for DES"

cipher alphabet is fixed throughout the encryption



Relative frequency of letters in english text

↓ so easy to break

Countermeasure :- Provide multiple substitute (homophones) for a single letter

Diagram
- Two letter combination

Tigram
- Three-letter combination

Playfair cipher

- Best known multiple-letter encryption cipher
- we use 5x5 matrix of letters
- Invented by british scientist Sir charles Wheatstone in 1854
- used by british & USA in world war-I & U.S Army & Allied forces in world war-II
  - → The sender and receiver decide on a particular key say tutorials
    - Fill in letters of keyword (minus duplicates) from left to right & top to bottom, then fill in the remainder of matrix with remaining letters in alphabetic order

eg:-

T	U	O	R	I
A	L	S	B	C
D	E	F	G	H
K	M	N	P	Q
V	W	X	Y	Z

→ First a plain text is split into Pairs of two letters (digraphs)
If there are odd number of letters a 'X' (or) 'Z' is added to last letter. Consider hide money

eg: HI DE MO NE YZ
(added)

Rules of encryption

1. If both letters are in the same coloumn, take letter below each one (going back to top if at the bottom)

eg:-

T	U	O	R	I
A	L	S	B	C
D	E	F	G	H
K	M	N	P	Q
V	W	X	Y	Z

HI → QC

2. If both letters are in same row take letter right to the each one (go back to left it at farthest right)

T	U	O	R	I
A	L	S	B	C
D	E	F	G	H
K	M	N	P	Q
V	W	X	Y	Z

DE → EF

3. If neither of preceding two rules are true, forms a rectangle with two letters on horizontal opposite corner of the rectangle.

T	U	O	R	I
A	L	S	B	C
D	E	F	G	H
K	M	N	P	Q
V	W	X	Y	Z

MO → NU

∴ hide money

→ QC EF NU MF ZV

It is relatively difficult to break, But cryptoanalysis is possible, 625 possible pairs of letters (25 × 25) instead of 26 different possible alphabets.

Hill cipher

– Lester Hill (1929)

Its a polygraphic substitution cipher Based on linear algebra. Each letter is represented by a number mod 26

eg: we have to encrypt message 'ACT' (n=3) and key = GYBNQKURP which can be written as matrix,

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}$$

Message ACT is

$$\begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix}$$

enciphered vector

$$= \begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix} \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix} \cdot \bmod 26 = \begin{bmatrix} 67 \\ 222 \\ 319 \end{bmatrix} \bmod 26 = \begin{bmatrix} 15 \\ 14 \\ 7 \end{bmatrix}$$

= POH

To decrypt the message we turn ciphertext back into a vector then simply multiply with key matrix inverse

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}^{-1} \begin{bmatrix} 15 \\ 4 \\ 7 \end{bmatrix} \bmod 26$$

$$\Rightarrow \begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix} \begin{bmatrix} 15 \\ 4 \\ 7 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 260 \\ 574 \\ 539 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix} \Rightarrow ACT$$

Polyalphabetic ciphers

- improves the simple monoalphabetic by using different substitutions as one proceeds through plain text.

All these techniques have common features

- A set of related Monoalphabetic Substitution rules is used
- A key determines which particular rule for given Transformation

Vigenere cipher [unbreakable]

- Best known and one of the simplest polyalphabetic substitution ciphers
- In this scheme the set of related monoalphabetic substitution rules consists of 26 caesar ciphers with shifts of 0 through 25.
- each cipher is denoted by a key letter which is the ciphertext letter that substitutes for plaintext letter a

26x26 matrix

eg:- Key depends on size of message
Size(key) = size (message)

- Keyword = deceptive
message = we are discovered save yourself
Key = deceptive deceptive deceptive
plain = wearediscovered saveyourself
cipher = ZICVTWQNGRZGVTWAVZHCQYGLMGJ

Vigenere Autokey system

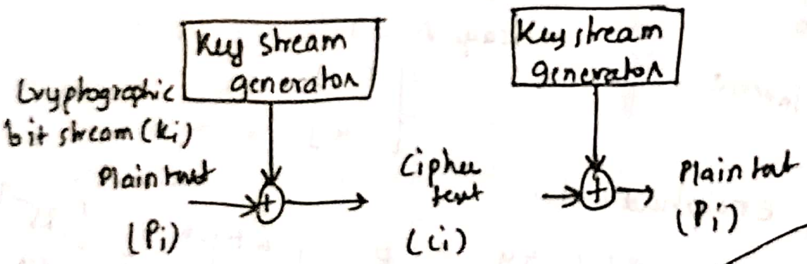
- A keyword is concatenated with plaintext itself to provide a running key
- even this is vulnerable to cryptoanalysis. [key the... chain can... frequency dis...]

Variants of vigenere cipher

(i) The Keyword length is same that of a plaintext message. It is Vernam cipher
more secure than vigenere cipher

(ii) one time pad : [Unbreakable Perfect secrecy]
→ length(key) = length...
→ Key is a random string of alphabets
→ Key is used only once
so each new message requires new key of same length of new message
Scheme is unbreakable

Vernam cipher



limitations / difficulties of one time pad

1. making large number of random keys [In practical require millions]
2. Mammoth Key distribution problem
– For every message to be sent, a key of equal length is needed by both sender & receiver.

Row Transposition cipher

more complex
write message in rectangle row by row, coloumn by coloumn, but permute the order of coloumns
Order of coloumns become key to algorithm

Transposition cipher

Rail fence cipher

simple Transposition cipher
plain text is written down as a sequence of diagonals and then read off as rows

eg: Msg = meet me after the toga party

m e m a t r h t g p r y
e t e f e t e o a a t

encrypted message is
...uetetetecoaat

eg::

(0-9)

key = 4312567

p = attack p
ostpone
duntilt
woamxyz

cipher text

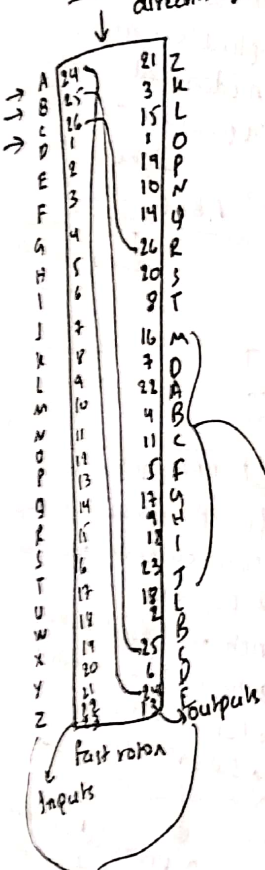
TTNAAPTMTSUOAODWCOIXKNLYPETZ

edbc
12

1	2	3	4	5	6	7

→ write in ascending or descending & write down.

Rotor machines



"It is a machine with multiple stages of encryption"

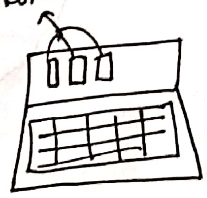
Consists of cylinders

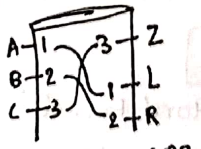
Security ∝ No. of cylinder

↓

There will be 26 inputs & 26 outputs to the cylinder → each input is associated with an alphabet

each input is internally connected to an output





So ABC → LR2

If one cylinder is used, it is vulnerable, multiple cylinders cannot be made vulnerable

↓

outputs of one cylinder will be connected to inputs of next cylinder

non Repetitive Inputs & outputs → Can make mapping to multilevel

↓

These cylinders will be rotating So after each key stroke it will make a shift

Steganography → Concealing one file, message .. within another file, message.

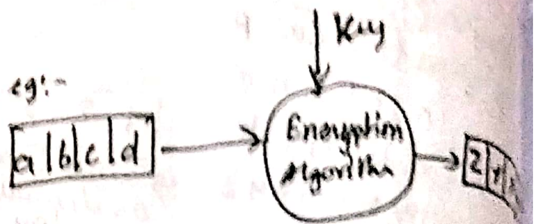
- Character Marking
  - Selected letters are Printed uniquely
  - marks are not visible until unless Paper is held at certain angle
- Invisible Ink
- Pin Punctures
- Typewriter Correction ribbon → not visible until unless under a strong light.

Information Security – I (iii)

Block cipher → encrypts & decrypts a block of data at a time
(symmetric)

↓ A block of plaintext is encrypted to produce a block of ciphertext of equal length

eg:-



In Block cipher
1. Plaintext is divided into fixed size blocks ✓
2. each block is encrypted ✓
3. The size of block is preferably large & a multiple of 8 ✓
4. If plaintext is not a multiple of block size, padding schemes can be applied ✓

↓
eg: P = DONTGIVEMONEY
let block size = 4

DONT	GIVE	MONE	Y

Note

- ciphertext of previous block is applied to next block
- even identical blocks will produce different ciphertext

eg: ABCD ABCD
↳ NVOP → used to encrypt next block

Block cipher examples

1. DES (Data encryption Standard)
2. AES (Advance encryption standard)
3. IDEA (International data encryption algorithm)
4. Triple DES
5. RC5 – Rivest cipher 5 (or) Ron's code 5 etc.

Claude Shannon introduced idea of (S-P) networks in 1949 which form basis for modern Block ciphers
→ SP nets are based on two cryptographic operations
- Permutation
- Substitution

↓
To provide confusion and diffusion

Confusion: makes relationship between key & ciphertext as complex as possible

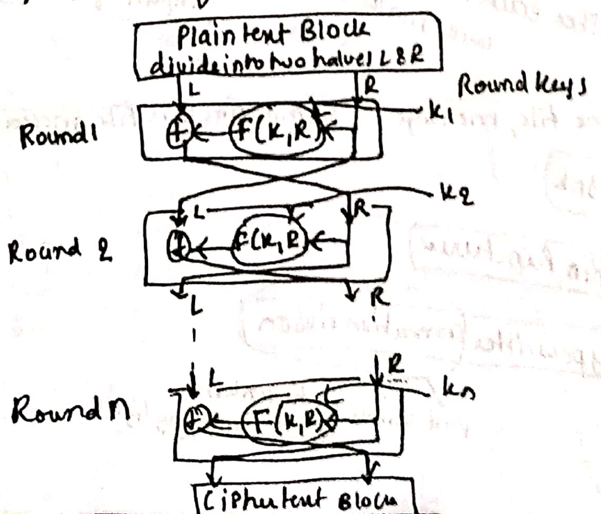
diffusion: dissipates the statistical structure of plaintext over bulk of ciphertext

Feistel Structure

– Horst Feistel

- A symmetric structure used to build block ciphers.

  eg: DES
- A number of encryption rounds
- A round function F
- A number of subkeys



Block cipher modes of operation

★ Learn for SEM

For different types of messages we need different modes of operation

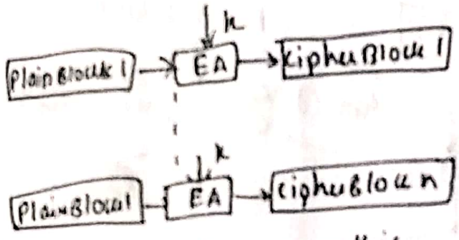
1. (ECB) mode Electronic codeBook
2. (CBC) mode Cipher Blockchaining
3. cipher Feedback mode (CFB) *
4. Output feedbacking mode (OFB) *
5. Counter (CTR) mode. *

OFB → same as CFB But in here output is feedback

CFB → we use Blockcipher as a streamcipher ↓ Plaintext is divided into segment of S(any) bits.

ECB mode

- simplest mode
- Plaintext is divided into number of fixed size blocks
- If message is not a multiple of blocksize then padding is done
- Takes one block at a time & encrypt it
- Same key used for encryption & decryption of each block



(X) But if identical blocks occur this Produces same ciphertext

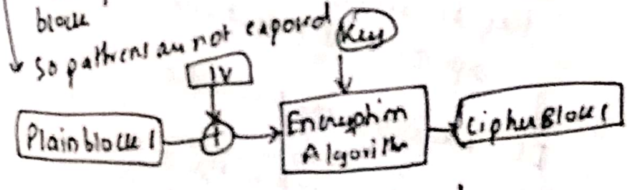
(X) Not secure for lengthy data

Counter Mode

- counter equal to plaintext block is used
- Counter is initialized to some value and incremented by 1 for each Subsequent block
- no chaining
- counter value need not to be Shared, but both need to be in synchronization.

(CBC) mode

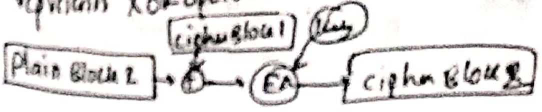
- overcome issue in ECB
- The input to encryption algorithm is the XOR of current plaintext block & the preceeding ciphertext block
- So patterns are not exposed



(X) If having two identical messages & if we use same IV then we get same cipher

IV → Initialization vector, used in first encryption & decryption

⊕ represents XOR operation



Data encryption standard (DES)

- widely used Block cipher in world
- encrypts 64 bit data using 56 bit key

DES History

IBM developed Lucifer cipher in late 1960s

↓

redeveloped by taking inputs from NSA

↓

In 1973 NBS Issued requests for proposals for national cipher standards

↓

IBM submitted revised Lucifer → DES

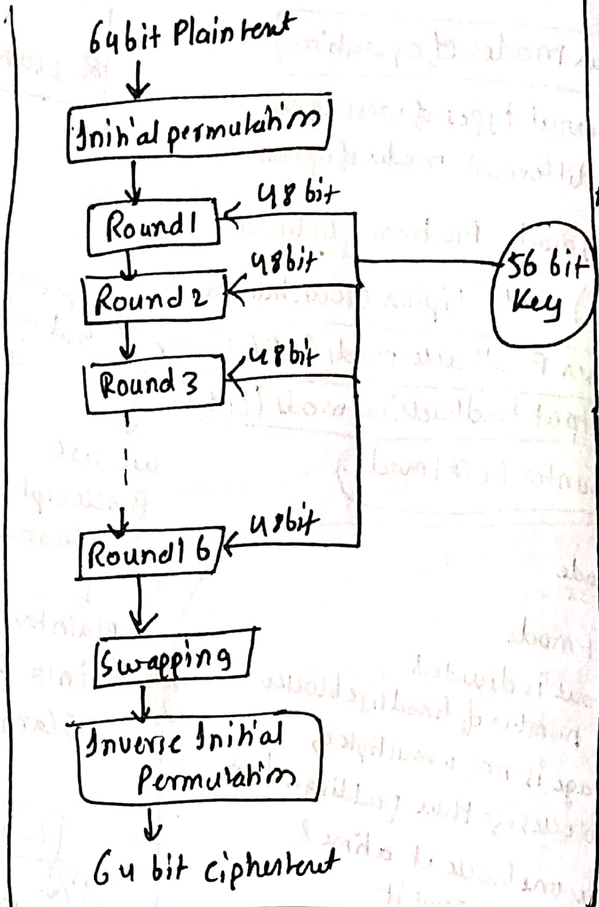
↓

eventually accepted

DES

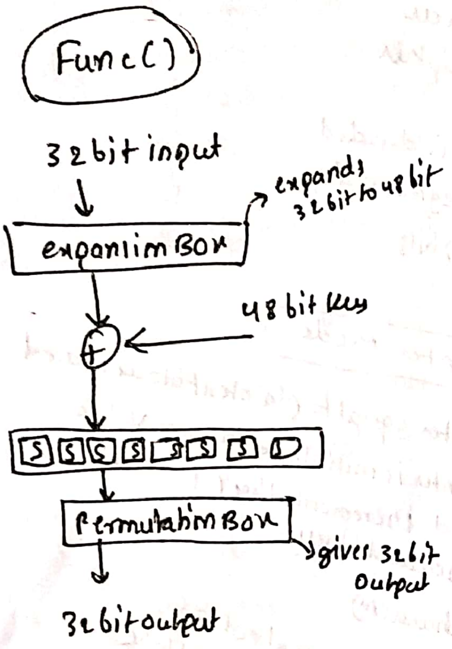
- 16 rounds
- 64 bit block size
- 56 bit key

→ Process of DES

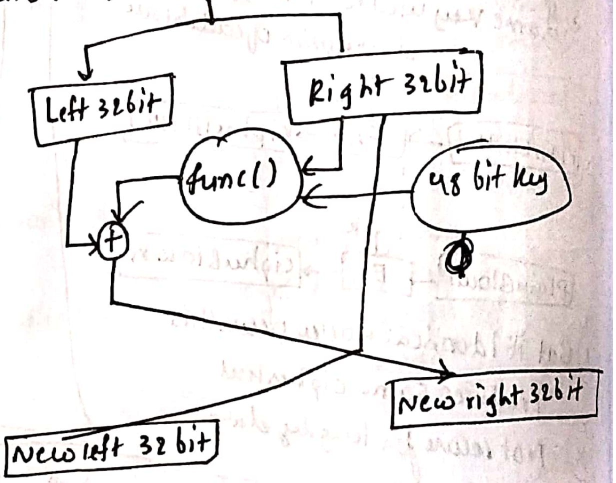


expansion permutation (learn later)

* 48bit key is used & other 8 bits are used for parity checking



In Round1 → 64 bit input



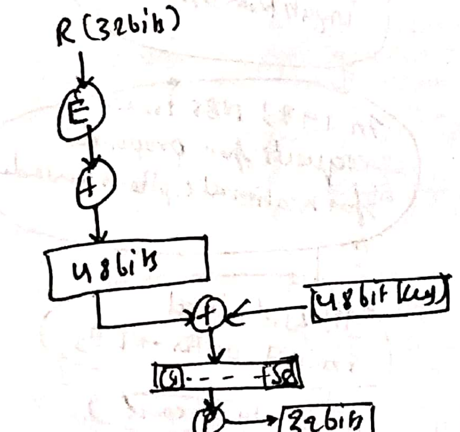
⊕ → XOR operation

To decrypt do the reverse procedure

DES Design Controversy

- 56 bit key vs (128 bit in Lucifer)
- DES was flourished in
  - financial applications

DES Round structure



Avalanche effect

- Key desirable property of encryption Algorithm.

↓

"where change of one input or key bit results in changing approx half output bits".

↓

DES exhibits strong Avalanche.

Strength of DES – key size

- 56 bit keys have $2^{56} = 7.2 \times 10^{16}$ values
- Brute force is hard

But you can still recognize the plaintext.

But Analytic Attacks can be done on DES

- By gathering information about encryptions
- Can eventually recover some/all of sub-key bits

↓

generally these statistical attacks include

- differential cryptanalysis
  ↓
  Analysing the behaviour of Pairs of text blocks evolving along each round of cipher.
- Linear cryptanalysis
  ↓
  attack based on finding linear approximation to describe the transformation performed in DES

AES | Advance encryption Algorithm

- Best & popular
- Block size = 128 bits (or 256)
- NO. of rounds depend upon key size

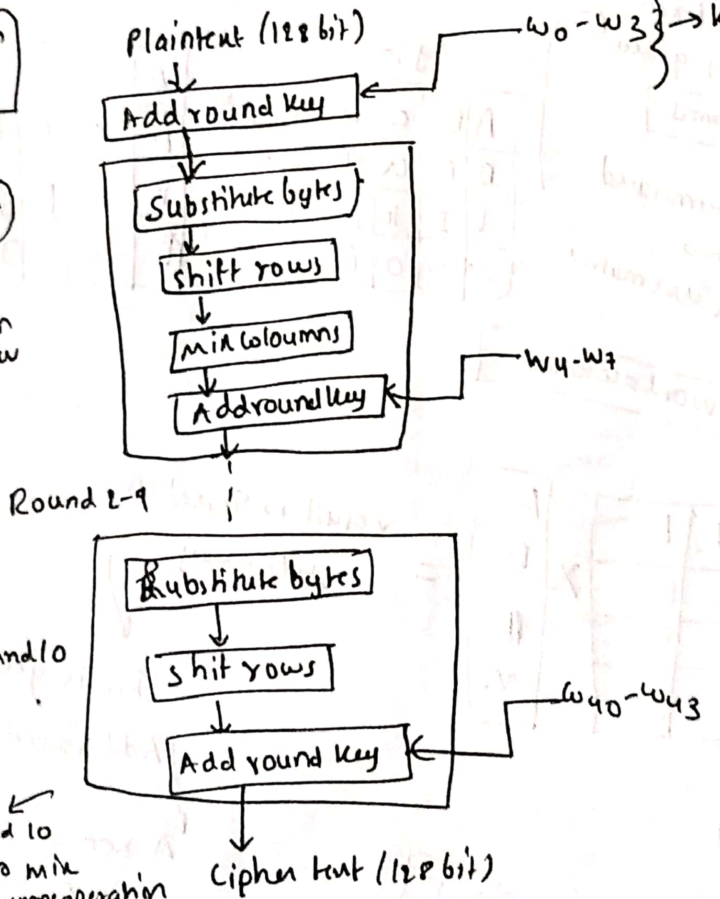
128 bit key - 10 rounds
192 bit key - 12 rounds
256 bit key - 14 rounds

- Data is processed as bytes not as bits
- So we have 128/8 = 16 bytes
- 4 bytes = 1 word
- Input is arranged in a 4x4 matrix

in0	in4	in8	in12
in1	in5	in9	in13
in2	in6	in10	in14
in3	in7	in11	in15

AES evaluation criteria

- Security
- cost
  - good computational efficiency
- Algorithm & implementation charateristics



In Round 10 There is no mix coloumn operation

↓

Intermediate results are stored in 4x4 matrix - state array

↓

output is also stored in an 4x4 matrix

↓

Key is stored in 4x4 matrix

W1 = k0k1k2k3
W2 = k4k5k6k7
W3 = k8k9k10k11
W4 = k12k13k14k15

Key is expanded to 44 words (w0 - - w43)

k0	k4	k8	k12
k1	k5	k9	k13
k2	k6	k10	k14
k3	k7	k11	k15

out0	out4	out8	out12
out1	out5	out9	out13
out2	out6	out10	out14
out3	out7	out11	out15

s00	s0,1	s02	s03
s10	s11	s12	s13
s20	s21	s22	s23
s30	s31	s32	s33

In round 1 → Substitute bytes use an s-box to perform byte by byte substitution

→ Take ino le 8bits

→ split into two halves

→ first half represents row and second half represents column

→ 16x16 sbox

→ Result will be sent to state array.

	0000	0001	— — —	1111
	.			
0001				
0010		11100101		
⋮				
1111				

input

output matrix from substitution stage will input to Shift rows

For first row noshift made

2nd row – 1 bytecircular left shift

3rd row – 2 byte circular Leftshift

4th row – 3 byte circular left shift

output from Shift rows is given to mix coloumns

eg:-

A	B	C	D
E	F	G	H
I	J	K	L
M	N	O	P

A	B	C	D
F	G	H	E
K	L	I	J
P	M	N	O

Take each coloumnand multiple with a Predefined 4x4 matrix

word = Coloumn

eg:-

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \times \begin{bmatrix} A \\ E \\ I \\ M \end{bmatrix} =$$

result is Stored in State array

This is given to Add roundkey stage

A XOR on State array is performed with first 4 words of key [ie, ex: w0 - w3] → 4 wordkey

ex:

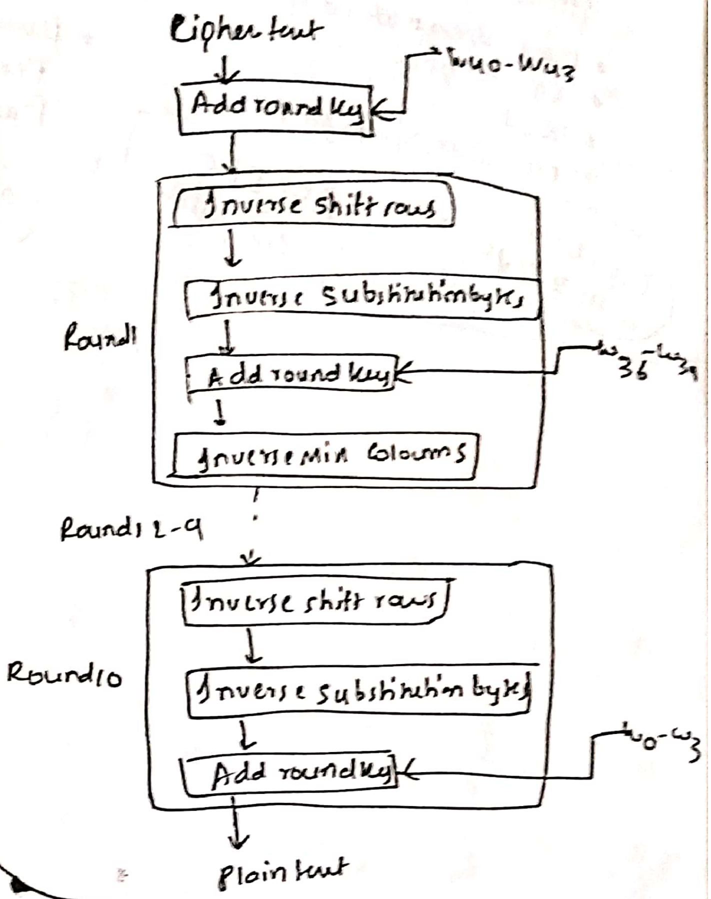
$$\begin{bmatrix} A & B & C & D \\ E & F & G & H \\ I & J & K & L \\ M & N & O & P \end{bmatrix} \oplus \begin{bmatrix} q & R & s & r \\ U & V & W & X \\ Y & Z & 1 & 2 \\ 3 & 4 & 5 & 6 \end{bmatrix}$$

result Stored in State array

In the round 10 there is no mix coloumns operation

AES decryption

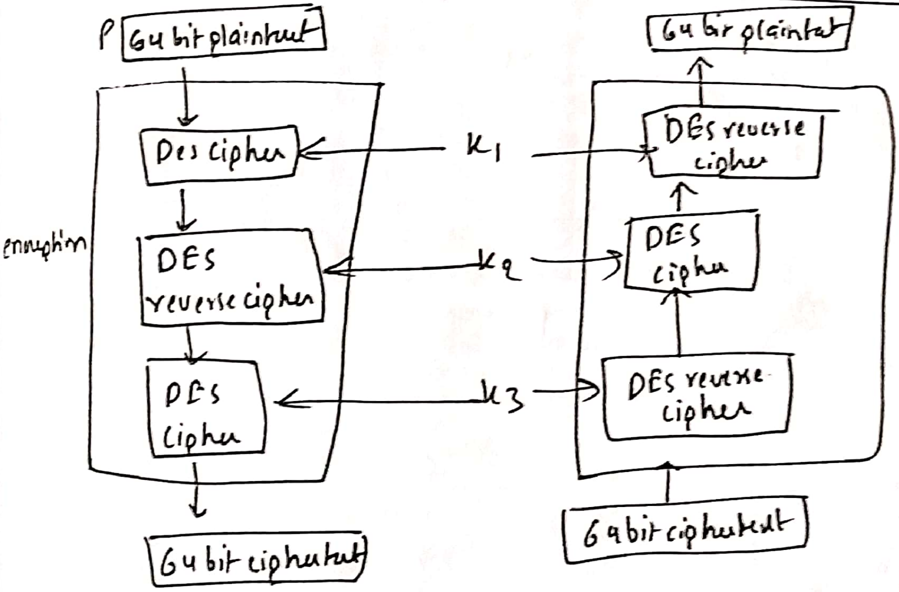
Just reverse!



3-Key Triple DES

- Key consists of 3 different keys k1, k2 k3
- 3×56 = 168 bits
- encrypt plaintext block with k1
- Now decrypt the output of above step with k2
- Now encrypt output of above step with k3
- The output is cipher text

In decryption use k3, k2 then k1



Stream cipher

which encrypts 1bit or 1byte at a time

Funpart Algorithm by Ron Rivest code revealed anamoly in mailing list in 1994 later revealed

RC4 Algorithm → variable key size byte oriented stream is used ↓ used in SSL, TSL, WEP

Psuedo random numbers Greators (PRNGs)

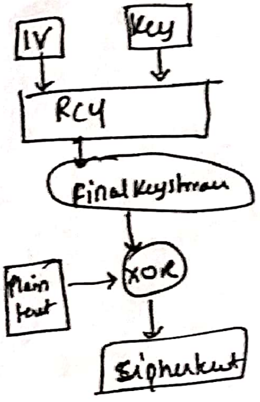
unpredictable

↓ source of true randomness

Conversion to binary

↓

Random bitstreams



IV
Key
RC4
Final Keystream
XOR
Plain text
Siphertext