26.06.12

Introduction

Security is a form of protection. Information is stored on the Computer. How can you assure that it is protected. When another user accesses it, there is a chance of reading the data, copying, modifying and even deleting it. (Even Viruses can be introduced in order to slow down the system.)* these are all forms of Attacks.

We need to restrict the user from logging in, or create separate user with Password protection. This can be treated as a mechanism to counter the attacks.

A Collection of tools designed to protect data and to thwart hackers is Computer Security.

When the Systems are distributed in a network, communication takes place among the nodes. Protection of data during transmission is Network Security.

Internet is a collection of large networks. Internet Security measures are needed to protect data during their transmission in the Internet.

Network Security (or) Internet Security consists of measures to deter, Prevent, detect and correct Security violations that involve the the transmission of information.

OSI (Open Systems Interconnection) Security Architecture

Def - OSI Security Architecture provides a frame work for defining Security Attacks, mechanisms and Services.

OSIA is a systematic way of defining the requirements for security and characterizing the approaches to satisfy those requirements. OSIA is useful to managers as a way of organizing the task of providing security.

Scanned by CamScanner

The OSI Architecture focuses on 3 aspects.

1. Security Attack : Any action that compromises the security of Information owned by an organization.
2. Security Mechanism : A process that is designed to detect, prevent or recover from a security attack.
3. Security Service : A processing or communication service that enhances the security of the data processing systems and Information transfers of an organization. The services are intended to counter security attacks, making use of security mechanism.

Threat : A potential for violation of security, when there is an action that could breach security and cause harm. Threat is a possible danger that might exploit a vulnerability.

Attack : An intelligent act or an attempt to evade security services and violate the security policy of a system.

Scanned by CamScanner

27.06.12

Securing Attacks: classified into Passive attacks and Active attacks

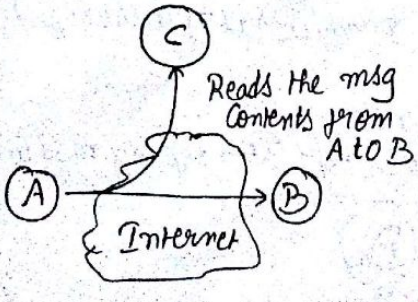
1) **Passive Attacks**: The opponents goal is to access the information that is being transmitted. but he doesn't make any changes to the normal flow of information, i.e. he doesn't the System resources are not affected. There are two types of Passive attacks. They are "release of message contents" and "traffic analysis".

a) **Release of message contents**: (Eavesdropping) Eg: A telephone Conversation, an email message containing Sensitive or Confidential information. (Prevent by encryption)

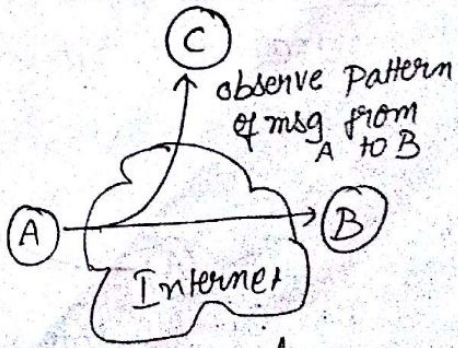
b) **Traffic Analysis**: (Monitoring): Encryption is the Solution of eavesdropping. An opponent might still be able to observe the pattern of these messages, determine the location, identity of communicating hosts. Could observe the frequency, length of messages being exchanged. This information might be useful in guessing the nature of the Communication that was taking place.

Passive attacks are difficult to detect as they do not involve any alteration of the data. Neither the Sender or the receiver is aware of that an opponent has read the message or observed the traffic pattern.

In this kind of attacks more emphasis is on Prevention rather than detection.



a) Release of message Contents

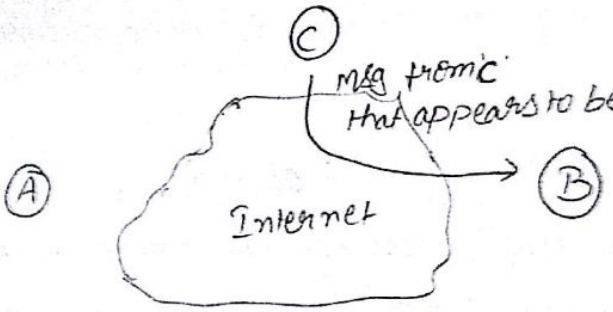


b) Traffic Analysis

Scanned by CamScanner

2) Active Attacks: An opponent or third party attempts to alter system resources or affect their operation. These are subdivided into four categories.

a) Masquerade: (False identity) this takes place when one entity pretends (acts) to be a different entity.

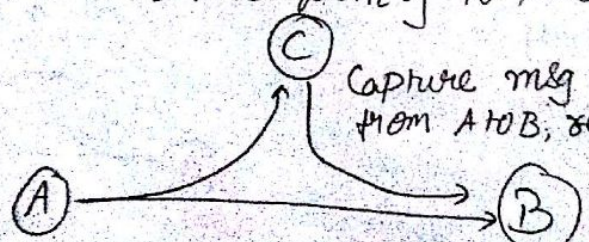


a) Masquerade

Eg: Authentication sequences can be captured and replayed after a valid authentication sequence has taken place, thus enabling an authorized entity with few privileges to obtain extra privileges by impersonating an entity that has these privileges.

Eg: Suppose you are opening a webpage of a website and trying to login into that, but it may be the intruder site. Unaware of this you may enter your userid and Pwd for authentication purpose. It is captured by the intruder and is the redirected to the actual site. Next time the intruder makes use of the userid and Pwd for authentication and acts as the original actual user. Now the intruders may be able to modify or delete the organizations critical data. gains privileges and

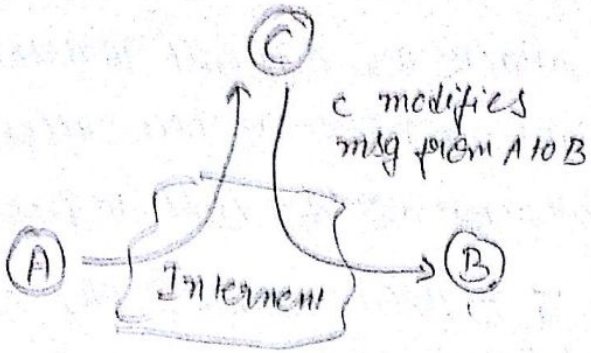
b) Replay: Captures the data while transmission and retransmits it subsequently to produce unauthorized effect. during



Eg: If A is sharing his key to B to prove his identity and C eavesdrop the conversation. Later C contacts to B and prove its

Scanned by CamScanner

c) Modification of messages: Some part of the legitimate message is altered or delayed or recorded to produce an unauthorized effect.

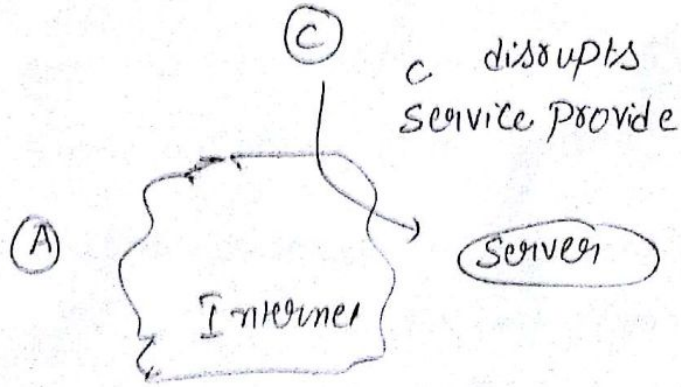


c) Modification of messages.

The attacker removes the msg from network traffic, alters it and reinserts it.

d) The denial of Serive : Prevents or inhibits the normal use or management of Communications facilities.

Eg : → Suppressing all msgs directed to a particular destination.
→ Disruption of an entire network either by disabling the network or by overloading it with msgs so as to degrade performance.



Eg : Inserting his own data into the data stream (Fabrication)
: playback of data from another Connection (Replay)
: Playback of data that had previously been sent in the same and opposite direction on the same Connection
: Deletion of Data
: man in the middle attack - The intruder sits in the middle of Communication link, intercepting msgs and

Scanned by CamScanner

Substituting them with his own messages. In this way, he tries to fool the parties to believe they are talking to each other directly, while they are really talking to the attacker.

Passive attacks are difficult to detect, but measures are available to prevent their success.

Active attacks are difficult to prevent because of the wide variety of ~~Physical~~ Potential physical, s/w and n/w vulnerabilities. These are easy to detect and the goal is to recover from any disruptions or delays caused by them.

Scanned by CamScanner

Security Services : A process that gives a specific kind of protection to the system resources. Security services implement security policies and are implemented by security mechanisms.

a) Authentication : Proving your identity.

Def : The assurance that the communicating entity is the one that it claims to be.

Ensuring that the origin of a msg is correctly identified

eg: Password

b) Access Control : Prevention of unauthorized use of a resource

c) Data Confidentiality : Protection of data from unauthorized disclosure. Ensuring that the data is accessible only (for reading) by authorized entities. No other parties can view the data. Confidentiality is the minimum requirement for n/w data transfer.

d) Data Integrity : The assurance that data received are exactly as sent by authorized entity.

(i.e. Contain no modification, insertion, deletion or replay)

e) Non-repudiation : Provides protection against denial by one of the entities involved in a communication.

Origin :- Proof that the msg was sent by the specified party.

Destination : Proof that the msg was received by the specified party.

f) Availability : is one that protects a system to ensure its availability. This service addresses the ~~sec~~ security concerns raised by denial-of-service attacks.

Scanned by CamScanner

Attack	Addressing Service	mechanism
1) Masquarade (forgery)	Authentication Non repudiation	~~Authentication exchange~~ Digital Signature
2) Replay	Authentication Non repudiation	~~Digital Signature Authentication Encipherment~~
3) Modification of msgs	Data Integrity	Data Integrity
4) Denial-of-service	Availability, Access Control	~~Data Integrity~~, ~~Authentication Exchange~~ Access Control
5) Release of msg Contents	Confidentiality	Encryption
6) Traffic Analysis	Confidentiality	Encryption & Traffic Padding

Security Mechanisms

1) Encipherment - Transformation of messages into an unintelligable form with the help of key.

2) Traffic padding - Insertion of bits into gaps in a data stream to frustrate traffic Analysis attempts

4)3) Digital Signature - Data appended to or a cryptographic transformation of a data unit that allows a ~~receip~~ recipient of the data unit to prove the source and integrity of the data unit and protect against forgery

5)4) Data Integrity : A mechanism used to assure the integrity of a data unit or stream of data units

3)5) Authentication Exchange : A mechanism intended to ensure the identity of an entity by means of information exchange.

6) Access Control : A variety of mechanisms that enforce access rights to resources

Scanned by CamScanner

Attack	Service	Mechanism
1. Release of msg contents	Confidentiality	Encipherment
2. Traffic Analysis	Confidentiality	Encipherment & Traffic Padding
3. Masquerade (forgery)	Authentication Non-repudiation	Authentication Exchange Digital Signature
4. Replay	Authentication Non-repudiation	Authentication Exchange Digital Signature
5. Modification of msg	Data Integrity	Data Integrity
6. Denial of Service	Availability Access Control	Authentication Exchang Access Control

Scanned by CamScanner

A Model for Network Security

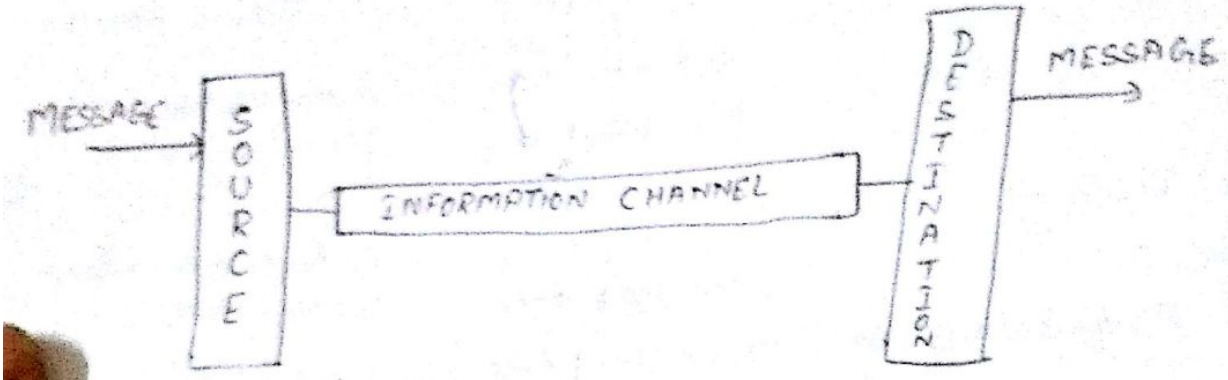
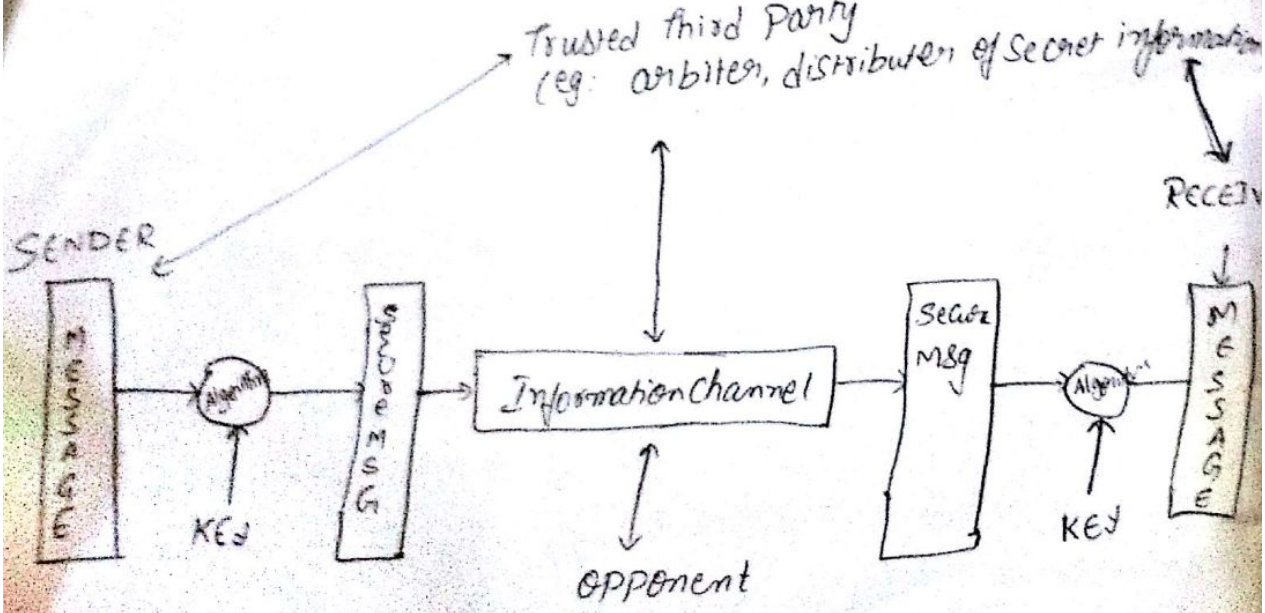


fig (a) MESSAGE TRANSMISSION



fig(b) Model for Network Security

In fig (a) we can observe that a message is being transmitted from Sender to Receiver. There is no security to the data because an opponent can also access the data as there are no security measures taken.

Now, comes into picture a Trusted Third Party as shown in fig (b).

Scanned by CamScanner

The Trusted Third party will help for secure data transmission with the help of a key.

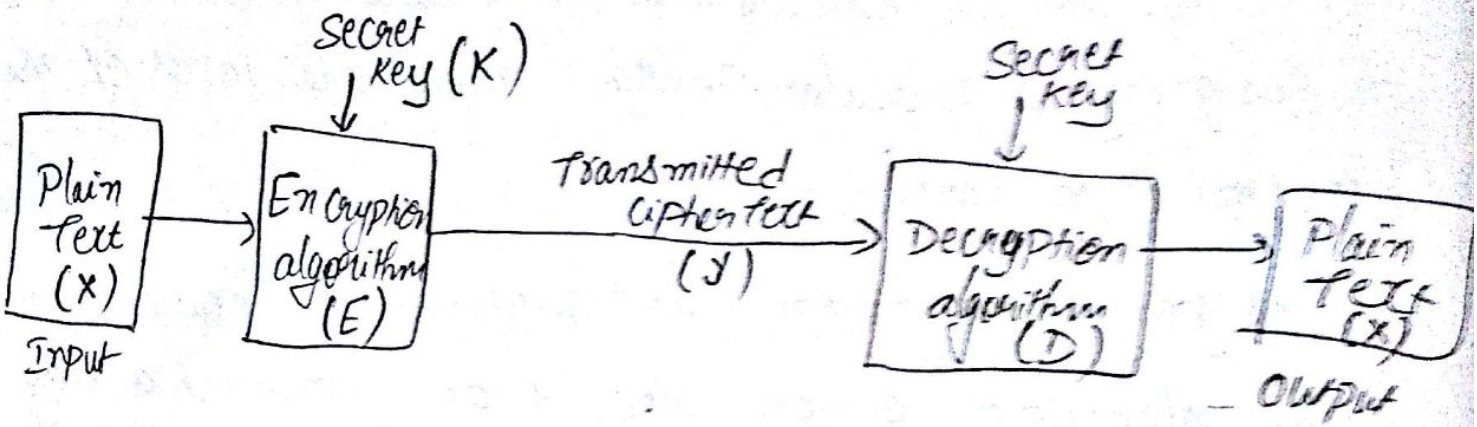
This model shows that there are 4 basic tasks in designing a particular service. These are tasks of the trusted third party.

1. Design an algorithm for performing secure-transmission. The algorithm design should be in such a way that the opponent cannot defeat its purpose.
2. Generate a secret information to be used along with the algorithm.
3. Develop methods for the distribution and sharing of secret information.
4. Specify a protocol to be used by the two principal entities that makes use of the security algorithm and the secret information to achieve a particular service.

The trusted third party is also called an arbiter. Which means the one who settles the disputes between the parties which are participating in the communication concerning the authentication of a message transmission.

Scanned by CamScanner

Symmetric Cipher Model



Simplified model of Encryption (Conventional)

X - Plain text
K - Key
E - Encryption Algorithm
Y - Cipher text
D - Decryption Algorithm

$$Y = E(K, X)$$

$$X = D(K, Y)$$

Scanned by CamScanner

Cryptography : The study of secure communications, dealing with the design of algorithms for encryption and decryption, intended to ensure the secrecy and/or authenticity of messages.

Cryptographic Systems are classified in 3 ways

1. The type of operations used for transforming plaintext to ciphertext :- All the encryption algorithms are based on two general principles :
   a) Substitution :- (each element in the plaintext is mapped into another element)
   b) Transposition :- (Rearrangement of elements / scrambling of elements in the plaintext)
2. The Number of keys used : If both the sender and the Receiver use the same key, the system is called as symmetric / single-key / secret-key / conventional encryption. If both S & R use different keys, the system is referred to as Assymmetric / two-key / public-key encryption.
3. The way in which the plain text is processed :
   a) Block cipher : Processes the input as one block of elements at a time, producing an output block for each input block
   b) Stream cipher : Processes the input elements continuously producing output one element at a time.

Scanned by CamScanner

Cryptanalysis : The process of attempting to discover the plaintext or key or both is known as cryptanalysis.

Brute-force attack : Trying all possible keys on the ciphertext until the plaintext is obtained. On average, half of all possible keys must be tried to achieve success.

Cryptanalytic Attacks : Based on the amount of information known to the cryptanalyst. The algorithm and the encryption algorithm and the ciphertext are known to the cryptanalyst in all kinds of cryptanalytic attacks.

i) Ciphertext only : In this type of attack the cryptanalyst has the least amount of information to work with. Only brute force approach is available to find the plaintext or key.

ii) Known plaintext : In some cases, one or more PTs as well as their encryptions may be captured by the cryptanalyst. or some PT patterns may be observed. Eg. If an encoded file always begins with the same pattern, or has standardized header, the analyst may be able to deduce the key on the basis of the way in which the known PT is transformed. Here one or more PT-CT pairs formed with the secret key.

iii) Chosen Plaintext : ~~Plaintext chosen by~~ PT chosen by cryptanalyst, together with its corresponding CT generated with the secret key.

Scanned by CamScanner

If the analyst is somehow able to get the source-system to insert into the system a message, then a chosen plaintext attack is possible.

Here the analyst chooses the PT. So he can pick patterns that can be expected to reveal the structure of key. Differential Cryptanalysis is an example of this strategy.

iv) Chosen Ciphertext: purported ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key.

If the opponent has temporary access to the decryption system, he can choose ciphertext and obtain the corresponding PT.

v) Chosen text – iii) & iv): PT & CT pairs, CT & PT pairs (Source System, Destination)

The chosen ciphertext & chosen text are less commonly employed.

Generally an encryption algorithm is designed to withstand a known plaintext. Only a weak algorithm fails to withstand a ciphertext only attack.

Either the CT can be secure in two ways

Unconditionally Secure - If the CT does not contain enough info to determine uniquely the corresponding PT.

Computationally secure:

→ Cost of breaking the cipher exceeds the value of the encrypted information.

→ The time required to break the cipher exceeds the useful lifetime of the information.

Scanned by CamScanner

Substitution techniques :- The letters of the plaintext are replaced by other letters or by numbers or symbols.

Some of the Substitution Techniques are

i) Ceaser Cipher
ii) monoalphabetic Cipher
iii) Playfair Cipher
iv) Hill cipher
v) Polyalphabetic Cipher
vi) one-time pad (Vernam)

i) Ceaser Cipher - This was the popular Substitution technique in olden days, as it was the simplest. It was by Julius Ceaser.

This cipher involves replacing each letter of a the alphabetswith the letter standing three places further down the alphabet.

Eg: A VERY GOODMORNING TO YOU ALL /
D YHUB JRRGPRUQLQJ WR BRX DOO

An algorithm can be expressed from this.

For each plaintext letter P, substitute the ciphertext letter C.

$$C = E(3, P)$$
$$= \text{[illegible]}$$
$$C = (3+P) \bmod 26$$

A shift may be of any amount, so that the general Ceaser Cipher algorithm is

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

where K ranges from 1 to 25.

The Decryption algorithm is

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

Scanned by CamScanner

Brute-force cryptanalysis is easily performed for a Ceaser cipher, by simply trying all the 25 possible keys

3 imp. characteristics that enabled to use a brute-force cryptanalysis are :

1. The encryption and decryption algorithms are known
2. There are only 25 keys to try. (Key space is very less)
3. The language of the plain text is known and easily recognizable.

To make the language of the PT unrecognizable, it may be compressed and then encrypted.

ii) Monoalphabetic Cipher : To improve Ceaser cipher, a random selection of characters is used. Any permutation of characters may be used for substitution. This increases the key space to 26! and eliminates brute force attack.

Here the cryptanalyst can calculate the frequency of each character (and obtain the percentage of frequency for corresponding characters) then match with standard English relative frequencies to easily obtain some characters.

Eg : If T appears a very less no. of times in cipher text, then it may be J, Q, X or Z because these are the least frequently used characters in English.

If P appears more no. of times in ciphertext then it may be E, T, or S because these are the most frequently used characters in English.

Scanned by CamScanner

iii) Playfair Cipher: Best known multiple ... cipher. It is a based on a 5×5 matrix of letters constructed using a keyword.

Eg: COMPUTER

1. Fill the 5×5 matrix with the characters of the keyword
   COMPUTER
2. Fill the remaining elements with A, B, C, ... not repeating the character if it exists in the keyword.

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

Encryption: Consider a plaintext "Hello" for encryption

Steps

i) Divide the PT into pairs (two letters). If the letters in the pair are the same then introduce a filler x in between them.

HE LX LO

ii) 'H' is substituted by the element in the same row which intersects the column of 'E'. So the element is 'F'

iii) 'E' is substituted by the element in the same row which intersects with the column of 'H'. It is 'A'.

H E L X
↓ ↓ ↓ ↓
F A N W

iv) If the pair of elements occur in the same column then Substitute it with a letter in the next row of the same column.

L O
↓ ↓
W E

v) If the pair of elements occur in the same row then Substitute it with a letter in the next column of the same row. eg: PU

U C (Cyclic)

Scanned by CamScanner

PT → HELXLO
CT → FANWWE
PT → HELXLO

WELCOMEX
OF KOMPWR
UNIVERSITY
MS

GITAM
GOOD GIRL
FMCF HDEN

Playfair cipher was for a long time considered unbreakable and was used by the British Army during WWI

Play Fair is relatively easy to break using the frequency analysis method, because it leaves much of the structure of plaintext. A few hundred letters of CT are generally sufficient.

Hill Cipher : It is also a multiletter Hill cipher, developed by the mathematician Lester Hill in 1929.

Here the encryption algorithm takes m successive PT letters and substitutes for them m ciphertext letters. The substitution is determined by m linear equations in which each character is assigned a numerical value (a = 0, b = 1. ... z = 25). For m = 3, the system can be described as follows.

$$C_1 = [(K_{11}P_1 + K_{12}P_2 + K_{13}P_3) \bmod 26$$
$$C_2 = (K_{21}P_1 + K_{22}P_2 + K_{23}P_3) \bmod 26 \quad \text{mod } 2$$
$$C_3 = (K_{31}P_1 + K_{32}P_2 + K_{33}P_3)] \bmod 26$$

This can be expressed in terms of column vectors and matrices:

$$\begin{pmatrix} C_1 \\ C_2 \\ C_3 \end{pmatrix} = \begin{pmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{pmatrix} \begin{pmatrix} P_1 \\ P_2 \\ P_3 \end{pmatrix} \bmod 26$$

or $C = KP \bmod 26$

Scanned by CamScanner

Eg① Consider the plain text "Pay more money" and key is

$$K = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$$

Let $m=3$ ($\because K$ is 3×3)

The first 3 letters of PT are P a y which are represented as P-15 a-0 y-24

So the vector is $\begin{bmatrix} 15 \\ 0 \\ 24 \end{bmatrix}$

The $C = KP \bmod 26$.

$$C = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \begin{bmatrix} 15 \\ 0 \\ 24 \end{bmatrix} \bmod 26$$

$$C = \begin{bmatrix} 375 \\ 819 \\ 486 \end{bmatrix} \bmod 26$$

$$C = \begin{bmatrix} 11 \\ 13 \\ 18 \end{bmatrix} \Rightarrow \begin{matrix} L \\ N \\ S \end{matrix} \qquad \begin{matrix} L = 11 \\ N = 13 \\ S = 18 \end{matrix}$$

∴ So the ciphertext for Pay is LNS

The entire ciphertext is LNSHDLEWMTRW

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

$P = D(K, C) = K^{-1}C \bmod 26$

$= K^{-1}(KP \bmod 26) \bmod 26$

$= P \bmod 26$

$= P$

Scanned by CamScanner

Eg ② Suppose "FRIDAY" is the Plain text encrypted using 2×2 Hill cipher and results PQCFKU as cipher text. Then find the key.

$C = KP \bmod 26$

$\begin{pmatrix} P \\ Q \end{pmatrix} = K \begin{pmatrix} F \\ R \end{pmatrix} \bmod 26 \quad \begin{pmatrix} C \\ F \end{pmatrix} = K \begin{pmatrix} I \\ D \end{pmatrix} \bmod 26$

$\begin{pmatrix} 15 \\ 16 \end{pmatrix} = K \begin{pmatrix} 5 \\ 17 \end{pmatrix} \bmod 26 \quad \begin{pmatrix} 2 \\ 5 \end{pmatrix} = K \begin{pmatrix} 8 \\ 3 \end{pmatrix} \bmod 26$

$\begin{pmatrix} 15 & 2 \\ 16 & 5 \end{pmatrix} = K \begin{pmatrix} 5 & 8 \\ 17 & 3 \end{pmatrix} \bmod 26$

$C = KP \bmod 26$

$K = CP^{-1} \bmod 26$

$\therefore P^{-1} = \begin{bmatrix} 5 & 8 \\ 17 & 3 \end{bmatrix}^{-1} = \frac{1}{15-136} \begin{bmatrix} 3 & -8 \\ -17 & 5 \end{bmatrix} \bmod 26$

$= -\frac{1}{121} \begin{bmatrix} 3 & 18 \\ -17 & 5 \end{bmatrix} \bmod 26$

If inverse of P

if P is not invertible, then a new version of P can be formed with additional PT-CT pairs until an invertible K is obtained.

$P^{-1} = \begin{bmatrix} 9 & 2 \\ 1 & 15 \end{bmatrix}$

So $K = \begin{bmatrix} 15 & 2 \\ 16 & 5 \end{bmatrix} \begin{bmatrix} 9 & 2 \\ 1 & 15 \end{bmatrix} = \begin{bmatrix} 137 & 060 \\ 149 & 107 \end{bmatrix} \bmod 26$

$K = \begin{bmatrix} 7 & 8 \\ 19 & 3 \end{bmatrix}$

This result can be verified by testing the remaining PT-CT pairs

Scanned by CamScanner

2.14 CT - JET JPG using Hill cipher with the key

inverse key $\begin{bmatrix} 5 & 1 \\ 2 & 7 \end{bmatrix}$ $K^{-1} = \begin{bmatrix} 5 & 1 \\ 2 & 7 \end{bmatrix}$

$K = [K^{-1}]^{-1}$

$$K = \begin{bmatrix} 5 & 1 \\ 2 & 7 \end{bmatrix}^{-1} = \frac{1}{ad-bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix} = \frac{1}{35-2}\begin{bmatrix} 7 & -1 \\ -2 & 5 \end{bmatrix} \text{ mod } 26$$

$$K = \frac{1}{33}\begin{bmatrix} 7 & -1 \\ -2 & 5 \end{bmatrix} \text{ mod } 26$$

So multiplicative inverse of 33 mod 26 is as follows

$33 = 26 \times 1 + 7$ — (1)

$26 = 7 \times 3 + 5$ — (2)

$7 = 5 \times 1 + 2$ — (3)

$5 = 2 \times 2 + 1$ — (4)

from eq (4) $1 = 5 - 2 \times 2$

" (3) $= 5 - 2 \times [7 - 5]$

$= 5 - 2 \times 7 + 2 \times 5$

$= 3 \times 5 - 2 \times 7$

" (2) $= 3 \times [26 - 7 \times 3] - 2 \times 7$

$= 3 \times 26 - 9 \times 7 - 2 \times 7$

$= 3 \times 26 - 11 \times 7$

" " (1) $= 3 \times 26 - 11 \times [33 - 26]$

$= 3 \times 26 - 11 \times 3 - 26 \times 11$

$1 = 14 \times 26 - 11 \times 33$

should be in this form.

$-11 \times 33 \text{ mod } 26$

$= -363 \text{ mod } 26$

$= 1$

This implies -11 is the multiplicative inverse of 33 mod 26

Scanned by CamScanner

Poly Alphabetic Cipher (Vigenere Cipher)

the cryptanalysis more harder to with more alphabets to guess and flatter frequency distribution.

Repeat the keyword, and place it above PT and encrypt to obtain CT using the table

	A	B	C	D
A	A	B	C	D
B	B	C	D	E
C	C	D	E	F
D	D	E	F	G

row → Key	BAD	BAD
Col → PT	BBC	ABC
CT	CBF	BBF

By determing the size of the key, cryptanalysis is reduced.

One Time Padding: Eliminate the repitions of the keyword by using a non-repeating random keyword equivalent to the size of PT. This is one-time padding and is unbreakable, because the CT does not contain any info about PT.

Practically it is difficult for generation and distribution random key, which cannot be be re-used for further transformations. So it is very rarely used where there are low band width channels requiring very high, security.

Scanned by CamScanner

Transposition Techniques : The letters are scrambled / mapped by performing some sort of permutation.

i) Rail Fence Technique : The PT is written down as a sequence of diagonals and then read as a sequence of rows.

eg: PT: WELCOME TO GITAM

W L O E O I A
E C M T G T M

CT : WLOEOIAECMTGTM

ii) A more complex scheme is to write the message, col by col, but permute the order of the columns. The order of the columns becomes the key of the algorithm.

PT WELCOME TO GITAM UNIVERSITY

4 3 1 2 5 7 6
W E L C O M E
T O G I T A M
U N I V E R S
I T Y W X Y Z

CT - LGIY CIVWEONT WTUIOTEXEMSZMARY

A pure transposition cipher can be easily recognised because of the same letter frequencies. This can be made more secure by performing more than one stage of transposition.

Scanned by CamScanner

Steganography: the ~~exact~~ methods of hiding the existence of a message

eg: The sequence of first letters of each word of the overall message forms the hidden message.

Examples of some Steganographic techniques that have been used historically are as follows:

i) Character marking: overwriting selected letters with pencil. visible only when the paper is held at an angle to a bright light.

ii) Invisible Ink: visible only when heat or some chemical is applied to the paper.

iii) Pin punctures: paper must be held up in front of a light to view the message.

iv) Type writer Correction Ribbon: visible ~~text~~ only under a strong light.

Steganography requires a lot of overhead to hide a few bits of info.

Cryptography	Steganography
1. Hides only the meaning but not the message	1. Hides the existence of a msg
2. Comparatively less time Consuming	2. Time Consuming
3. Less overhead	3. Lots of overhead for a few bits of info
4. Used for transmitting Secret info.	4. Used by Secret Communicators
5. Eg: Substitution, Transposition Techniques	5. Invisible ink, Pin Punctures etc.

Scanned by CamScanner

Hill Cipher Encryption

$K = -11\begin{bmatrix} 7 & -1 \\ -2 & 5 \end{bmatrix} \bmod 26 = \begin{bmatrix} -77 & 11 \\ 22 & -55 \end{bmatrix} \bmod 26 = \begin{bmatrix} 1 & 11 \\ 22 & 23 \end{bmatrix}$

$K = \begin{bmatrix} 1 & 11 \\ 22 & 23 \end{bmatrix}$ $\quad K^{-1} = \begin{bmatrix} 5 & 1 \\ 2 & 7 \end{bmatrix}$

Deciphering

$\begin{bmatrix} y \\ I \end{bmatrix} \rightarrow \begin{bmatrix} 24 \\ 8 \end{bmatrix}$ $\quad P = K^{-1}C \bmod 26$

$= \begin{bmatrix} 5 & 1 \\ 2 & 7 \end{bmatrix} \begin{bmatrix} 24 \\ 8 \end{bmatrix} \bmod 26 = \begin{bmatrix} 5\times24+1\times8 \\ 2\times24+7\times8 \end{bmatrix} \bmod 26 =$

$= \begin{bmatrix} 128 \\ 104 \end{bmatrix} \bmod 26 = \begin{bmatrix} 24 \\ 0 \end{bmatrix} \Rightarrow \begin{bmatrix} y \\ a \end{bmatrix}$

Verification

PT $\begin{bmatrix} y \\ a \end{bmatrix} \rightarrow \begin{bmatrix} 24 \\ 0 \end{bmatrix}$ $\quad C = KP \bmod 26$

$= \begin{bmatrix} 1 & 11 \\ 22 & 23 \end{bmatrix} \begin{bmatrix} 24 \\ 0 \end{bmatrix} \bmod 26 = \begin{bmatrix} 24+0 \\ 528+0 \end{bmatrix} \bmod 26 = \begin{bmatrix} 24 \\ 8 \end{bmatrix}$

Deciphering

$CT = \begin{bmatrix} T \\ J \end{bmatrix} \rightarrow \begin{bmatrix} 19 \\ 9 \end{bmatrix}$ $\quad P = K^{-1}C \bmod 26$

$= \begin{bmatrix} 5 & 1 \\ 2 & 7 \end{bmatrix} \begin{bmatrix} 19 \\ 9 \end{bmatrix} \bmod 26 = \begin{bmatrix} 5\times19+1\times9 \\ 2\times19+7\times9 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 95+9 \\ 38+63 \end{bmatrix} \bmod 26 = \begin{bmatrix} 104 \\ 101 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 0 \\ 23 \end{bmatrix} \rightarrow \begin{bmatrix} a \\ x \end{bmatrix}$ PT

Verification

$PT \rightarrow \begin{bmatrix} a \\ x \end{bmatrix} \rightarrow \begin{bmatrix} 0 \\ 23 \end{bmatrix}$ $\quad P = K^{-1}C \bmod 26$

$= \begin{bmatrix} 5 & 1 \\ 2 & 7 \end{bmatrix} \begin{bmatrix} 0 \\ 23 \end{bmatrix} \bmod 26 = \begin{bmatrix} 5\times0+1\times23 \\ 2\times0+7\times23 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 0+23 \\ 0+ \end{bmatrix}$

$C = KP \bmod 26$

$= \begin{bmatrix} 1 & 11 \\ 22 & 23 \end{bmatrix} \begin{bmatrix} 0 \\ 23 \end{bmatrix} \bmod 26 = \begin{bmatrix} 1\times0+11\times23 \\ 22\times0+23\times23 \end{bmatrix} \bmod 26 = \begin{bmatrix} 253 \\ 529 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 19 \\ 9 \end{bmatrix} \rightarrow \begin{bmatrix} T \\ J \end{bmatrix} \rightarrow CT$

Scanned by CamScanner

Block Cipher Principles

Stream Cipher: is one that encrypts a digital data stream one bit or one byte at a time. Eg: autokeyed Vigenere Cipher (Polyalphabetic) and the Vernam cipher (one time pad)

Block Cipher: is one in which a block of PT is treated as a whole and used to produce a cipher text block of equal length. Generally a block size of 64 or 128 bits is used.

Majority of network-based symmetric cryptographic applications make use of block ciphers.

Motivation for the Feistel Cipher Structure

A block cipher operates on a PT block of n bits to produce a CT block of n bits. So there are 2^n possible different plaintext blocks. Each PT block must produce a unique CT block for the encryption to be reversible (also called nonsingular)

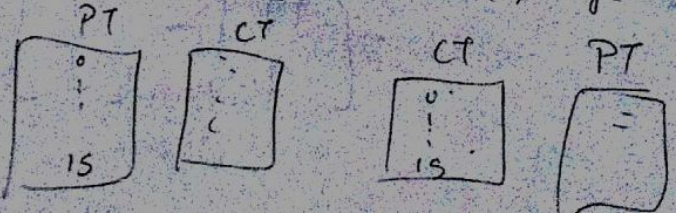
Reversible Mapping

PT	CT
00	11
01	10
10	00
11	01

Irreversible Mapping

PT	CT
00	11
01	10
10	01
11	01

For a general Substitution cipher of $n = 4$, there are 16 4-bit i/ps which map uniquely to 16 possible o/p states each of which are 4bit CT. We can ~~represent~~ define the encryption and decryption mappings



Scanned by CamScanner

This is the general form of block cipher and Feistel refers to this as the "ideal block cipher". A substitution cipher for $n = 4$ is vulnerable to a statistical analysis of the PT, as the because of small block size. If n is sufficiently large, the statistical characteristic of the PT is masked and cryptanalysis is infeasible.

But large block size is not practical from implementation and performance point of view. For such a transformation, the mapping itself constitutes the key. Then the required key length is 4 bits × 16 rows

= 64 bits.

In general, for an n-bit ideal block cipher, the key length is defined as $n \times 2^n$ bits. For $n = 64$,

~~$64 \times 2^{64} = 2^6 \times 2$~~

$64 \times 2^{64} = 2^6 \times 2^{64} = 2^{70} \approx 10^{21}$ bits.

Feistel points out that an ideal block cipher system (approximation to the) for large n is needed. ~~This~~ He proposed the concept of a Product cipher which is the execution of two or more simple ciphers in sequence so that the final result or product is cryptographically stronger than any of the component ciphers. Claude Shannon developed a product cipher that alternates confusion & diffusion functions to frustrate the statistical cryptanalysis.

Till now we observed that frequency analysis and statistical analysis reflected by the CT have let the cryptanalyst to deduce the PT or key.

Shannon's idea is to develop a strongly ideal cipher. in such a way that all statistics of CT are independent of the particular key used.

Scanned by CamScanner

In diffusion, each PT digit affects the value of many cipher text digits, by which the statistical structure of the PT is dissipated into long-range statistics of the CT. (simply each CT digit is affected by many PT digits)

Diffusion can be achieved by repeatedly performing some permutation on the data followed by applying a function to that permutation, the effect is that bits from different positions in the original PT contribute to a single bit of CT.

Diffusion makes the statistical relationship between the plaintext and ciphertext as complex as possible

Confusion makes the statistical relationship between the CT & key as complex as possible. This is achieved by use of a complex substitution algorithm.

Diffusion hides the relationship between the ciphertext and plaintext
Confusion hides the relationship between the ciphertext and the key

Scanned by CamScanner

Diffusion and confusion can be achieved using iterated Product ciphers where each iteration is referred to as a round and it is a combination of S-boxes, P-boxes and other components. The blocked cipher uses a keygeneration to create diff. keys for each round from the cipher key. In an N-round cipher, the PT is encrypted N times to create CT, the CT is decrypted N times to create the PT. The text in b/w the rounds is called as middle text.

The fig in previous page shows a simple product cipher with 2 Rounds. Three transformations happen at each round:

a. The 8-bit text is mixed with the round key (to hide the text) ~~but~~ by exclusive-oring the 8 bit PT with 8-bit K

b. The o/ps of key mixer is grouped into four 2-bits and given as i/ps to 4 S-boxes. The values of bits are changed based on the structure of the S-boxes.

c. The o/ps of S-box are passed to P-box to transpose the bits so that in the next round each box receives diff. i/ps

Diffusion: Let us see how changing a single bit in PT affects multiple bits in the CT.

a. In the first round consider bit 8. It is ex-ored with the 8th bit of K_1 and goes as i/p to S-box 4 as i/p and affects 7th & 8th bits. When these bits in the P-box permute to 2nd & 4th bits respectively. So, after 1st round 8th bit of PT affects 2nd & 4th bits. In the second round, bit 2 goes to S-box 1, ~~bit~~ and bit 4 to S-box 2. So bits 1, 2, 3, 4 are affected and permute to 6, 1, 3, 7. So after the second round we can observe that bit 8 of the PT has affected bits 1, 3, 6 & 7.

b. We can consider this scenario in another direction i.e. from CT to the PT. This shows that each bit in the CT is affected by several bits in the PT.

Scanned by CamScanner

Confusion : The four bits of CT 1, 3, 6 & 7 are affected by 5 three bits in the key i.e. bit 8 in K, and bits 2 & 4 in K2. In the other direction we can observe that each bit in each round key affects several bits in the CT.

The relationship between CT & key bits is obscured.

Practical ciphers use large data blocks, more S-boxes and more rounds to improve diffusion & Confusion.

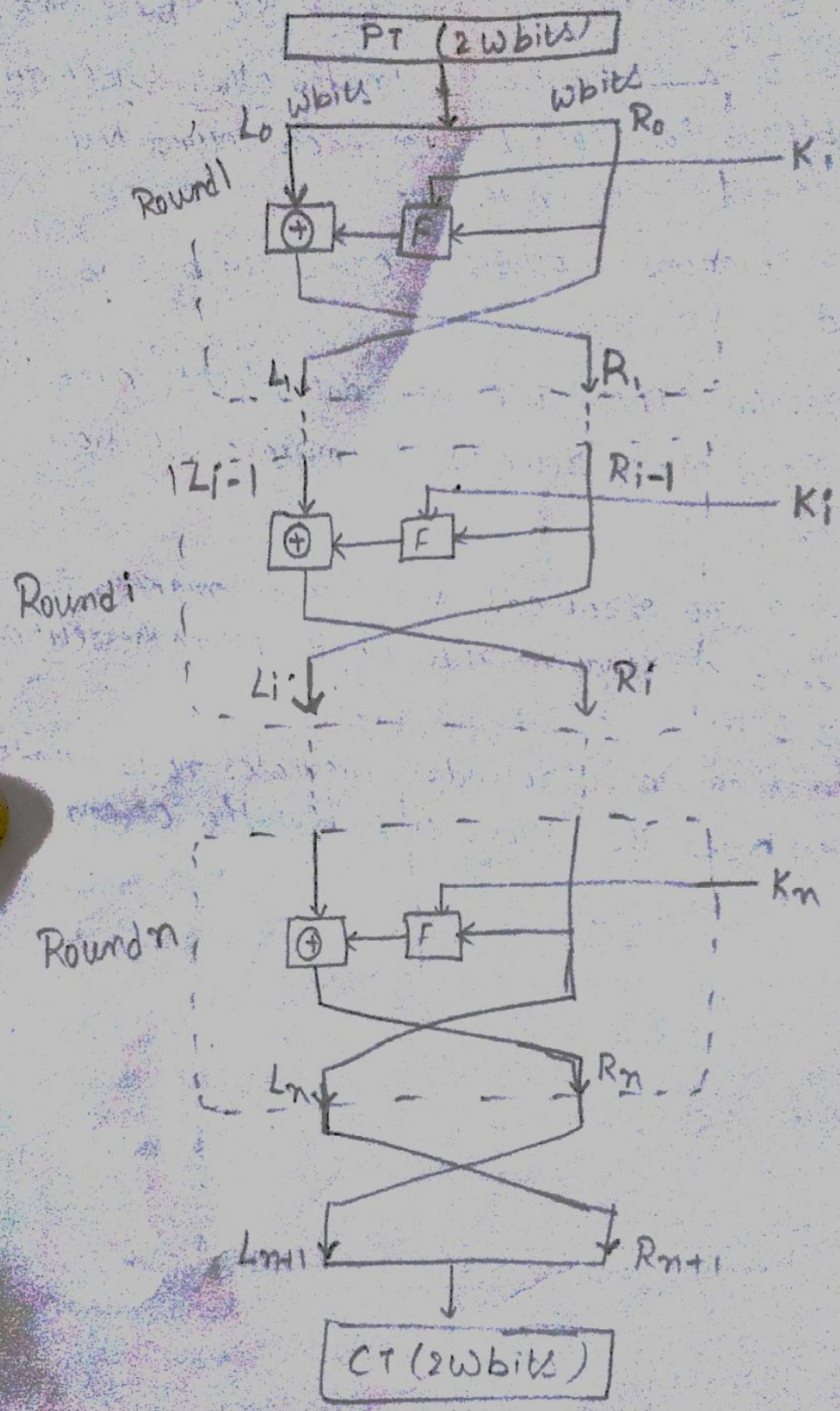
Increasing no. of rounds & S-boxes makes the CT look like a random n-bit word, hiding the relation b/w CT & PT.

Increasing no. of rounds increases no. of roundkey which better hides the relationship b/w the CT and the key.

Scanned by CamScanner

Feistel Cipher Structure

fig Classical Feistel Network



Let LE_i & RE_i denote the o/p of each encryption round of i^{th} block. So $LE_i = RE_{i-1}$

$$RE_i = LE_{i-1} \oplus F(K_i, RE_{i-1})$$

At the end of 16^{th} round the o/p is given by

$$LE_{16} = RE_{15}$$

$$RE_{16} = LE_{15} \oplus F(K_{16}, RE_{15})$$

Scanned by CamScanner

Encryption:
The figure shows the structure proposed by Feistel. The inputs to the encryption algorithm are Plaintext block of length 2w bits and a key K. PT block is divided into two halves, L_0 and R_0, they pass through n rounds of processing and then combine to produce CT block. Each round i has as inputs L_{i-1} and R_{i-1}, from the previous round and a subkey K_i generated from the cipher key K. Each K_i is unique.

Rounds: All rounds have the same structure. A substitution is performed on left half L_i with the o/p of Round function F. F is applied to the right half R_i of the data along with the round key K_i. Following this substitution, a permutation is performed by swapping the two halves. This structure is a particular form of substitution-permutation network (SPN) proposed by Shannon.

Decryption: It is similar to the encryption process. ~~PT~~ Cipher text is given as inputs to the algorithm, Subkeys K_i are given in reverse order. K_n in first round,..., ~~K_1 is~~ K_1 in the last round.

Block Cipher Design Principles: A Feistel network depends on the following parameters and design features.

1) Block size: Larger block sizes improves security, by greater diffusion but reduces encryption/decryption ~~speed~~ speed for a given algorithm. 64 bits block size has been considered a reasonable trade off.

2) Key size: Larger key size, greater confusion, greater resistance to brute force attack, but encryption/decryption speed may decrease. 128 bits has become a common size.

3) No. of rounds: multiple rounds offer increasing security. A typical size is 16 rounds.

Scanned by CamScanner

4) Subkey Generation algorithm : Greater Complexity in this algo. should lead to greater difficulty of Cryptanalysis.

5) Round function : Again, greater Complexity means greater resistance to Cryptanalysis

6) Fast Software encryption/decryption : Speed of execution of algorithm is a concern where encryption is embedded in applications to replace hardware implementations

7) Ease of analysis : Easy is the algorithm, more easier to analyze that algorithm for Cryptanalytic Vulnerabilities, so a highly strong algorithm has to be designed to make the analysis complicated.

Decryption in ciphers based on the Feistel Structure

→ Decryption alg is same as encryption alg but the keys are applied in reverse order.

→ The o/p of each round during ~~encry~~ decryption is the i/p to the corresponding round during encryption. This property holds true regardless of the choice of the Feistel function F.

→ Proof * Let LD_i & RD_i denote the left and right halves of the o/p of the i^{th} round.

* o/p of 1st round is LD_1 RD_1,
  i/p of 1st round is LD_0 RD_0.

The relationship between the ~~i/p~~ ~~inputs~~ inputs to the first decryption round and o/p of the encryption algorithm is

$$LD_0 = RE_{16}$$
$$RD_0 = LE_{16}$$

* o/p of 1st Decryption round is LD_1, RD_1

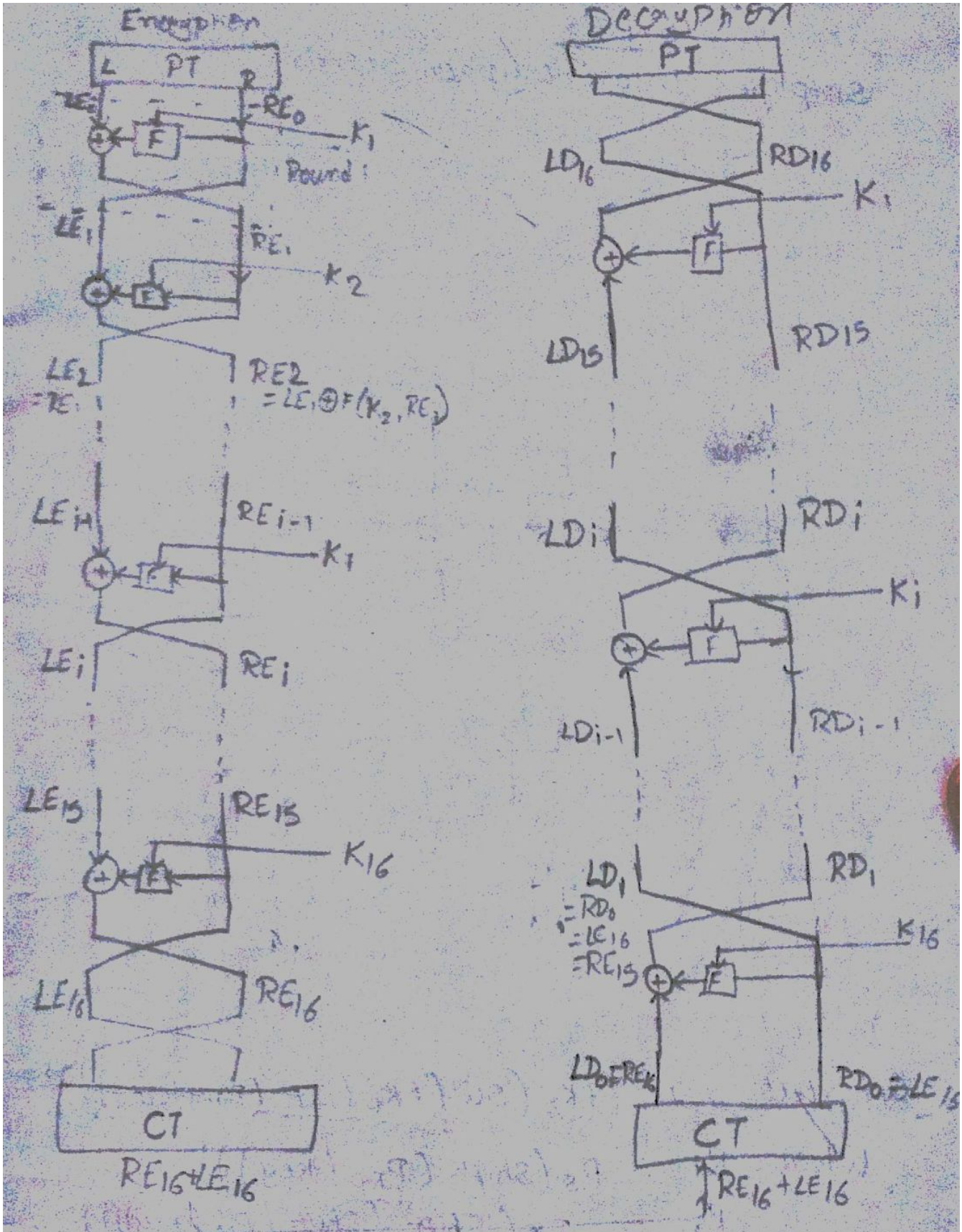
$$LD_1 = RD_0 \Rightarrow LE_{16} \Rightarrow RE_{15}$$

$$RD_1 = LD_0 \oplus F(K_{16}, RD_0)$$
$$= RE_{16} \oplus F(K_{16}, LE_{16})$$
$$= LE_{15} \oplus F(K_{16}, RE_{15}) \oplus F(K_{16}, RE_{15})$$
$$RD_1 = LE_{15}$$

$A \oplus B \oplus C = A \oplus B \oplus C$

$A \oplus A = 0$
$A \oplus 0 = A$

Scanned by CamScanner



Block Diagram of Feistel Cipher Structure for encryption & Decryption

$\therefore LD_1 = RE_{15} \Rightarrow LD_i = RE_{16-i}$

$RD_1 = LE_{15} \Rightarrow RD_i = LE_{16-i}$

The above result is independent of the precise nature of F.

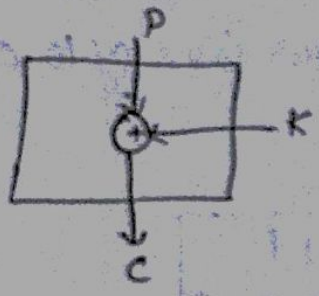
Scanned by CamScanner

Differential & Linear Cryptanalysis

This is a chosen-plaintext attack and the idea was introduced by Eli Biham and Adi Shamir. A somehow gets access to B's system. A chooses a set of PTs and obtains the corresponding CTs. Now the goal of A is to find B's cipher key.

Algorithm Analysis : The encryption algorithm is first analysed inorder to collect some info about PT-CT relationships. Some ciphers have weaknesses in their structure, this allows A to find the relationship b/w PT differences and CT differences without knowing the key.

Ex.



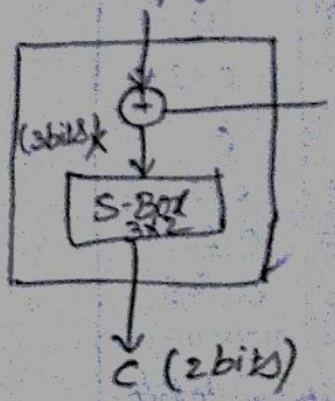
$C_1 = P_1 \oplus K_1 \quad C_2 = P_2 \oplus K_2$

Finding the relation b/w PT & CT differences

$C_1 \oplus C_2 = P_1 \oplus K \oplus P_2 \oplus K$

$C_1 \oplus C_2 = P_1 \oplus P_2$

Practically the cipher is not so simple, so add one S-Box



X	000	001	010	011	100	101	110	111
C	11	00	10	10	01	00	11	00

$X_1 \oplus X_2 = P_1 \oplus P_2$. Now S-Box prevents A to find the definite relation b/w PT & CT differences. But a Probabilistic relation can be created as shown in the Table. The table shows for each PT difference, how many CT differences the cipher may create.

Key size is 3 bits so 8 combinations can be obtained for each diff in the i/p.

Scanned by CamScanner

$C_1 \oplus C_2$

$P_1 \oplus P_2$	00	01	10	11
000	8			
001	2	2		4
010	2	2	4	
011		4	2	2
100	2	2	4	
101		4	2	2
110	4		2	2
111			2	6

Table shows that for the i/p diff. 000 the o/p diff is always 00. For the i/p diff. of 100 there are two cases of 00, two ~~Caseses~~ of 01, four cases of 10 o/p diff

$C_1 \oplus C_2$

$P_1 \oplus P_2$	00	01	10	11
000	1	0	0	0
001	0.25	0.25	0	0.5
010	0.25	0.25	0.5	0
011	0	0.5	0.25	0.25
100	0.25	0.25	0.5	0
101	0	0.5	0.25	0.25
110	0.5	0	0.25	0.25
111	0	0	0.25	0.75

Differential distribution table

(or)

XOR Profile.

Launching a chosen-Plain Text Attack : Now A chooses some PTs with highest Probability for attack.

Scanned by CamScanner

Ex: A knows that

if $P_1 \oplus P_2 = 001$ then $C_1 \oplus C_2 = 11$ with 3/4 Probability

Now A tries $C_1 = 00$ and gets $P_1 = 010$ (chosen plaintext attack)

" " $C_2 = 11$ and gets $P_2 = 011$

$C_1 = 00$ for $X_1 = 001$ or $X_1 = 111$

If $X_1 = 001$ then $K = X_1 \oplus P_1$ ⇒

$X_1 \to 001$
$P_1 \to 010$
011

&

If $X_1 = 111$ then $K_1 = X_1 \oplus P_1$ ⇒

$X_1 \to 111$
$P_1 \to 010$
111

If X_2

$C_2 = 11$ for $X_2 = 000$ and $X_2 = 110$

If $X_2 = 000$ $K = X_2 \oplus P_2$ ⇒

000
011
011

If $X_2 = 110$ $K_2 = X_2 \oplus P_2 =$

110
011
101

Now, even though the exact key value is not found we can observe that the rightmost bit is 1. More attacks can reveal more bits in the key.

Procedure: Modern ciphers have more complexity, than the above. They are also made from diff. rounds.

1. A can create a separate distribution table for each S-box and combine to create the distribution table for each round.
2. A can create a distribution table for the whole cipher

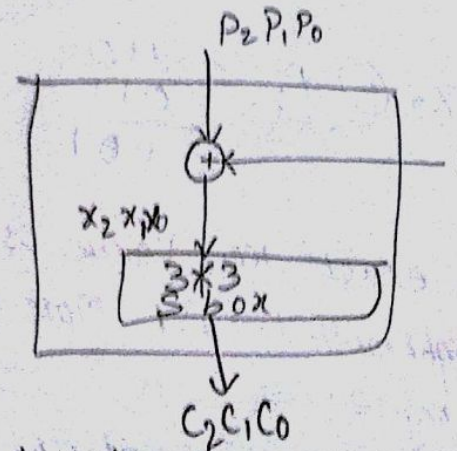
Scanned by CamScanner

3. A can now select of a set of PTs for attack with highest probability.
4. A chooses a CT and finds the corresponding PT and tries to find some bits in the key.
5. The step 4 has to be repeated to find more no. of bits in the key.
6. After finding enough no. of bits in the key, A can use brute force attack to find the whole key.

Differential cryptanalysis is based on a non-uniform differential distribution table of the S-boxes in a block cipher.

Linear Cryptanalysis: This was presented by Mitsuru Matsui in 1993. The analysis uses known PT attacks.

Assume a cipher is made of a single round where C_0, C_1, C_2 are O/P bits x_0, x_1, x_2 are i/p bits of S-box.



$C_0 = x_0 \oplus x_1$
$C_1 = x_0 \oplus x_1 \oplus x_2$
$C_2 = x_1 \oplus x_2$

S-box.

The S-box is a linear transformation in which each o/p is a linear fn of i/p. Three linear equations b/w PT & CT bits are given.

$$C_0 = P_0 \oplus K_0 \oplus P_1 \oplus K_1$$
$$C_1 = P_0 \oplus K_0 \oplus P_1 \oplus K_1 \oplus P_2 \oplus K_2$$
$$C_2 = P_1 \oplus K_1 \oplus P_2 \oplus K_2$$

Scanned by CamScanner

solving the three unknowns

$$K_1 = (P_1) \oplus (C_0 \oplus C_1 \oplus C_2)$$
$$K_2 = (P_2) \oplus (C_0 \oplus C_1)$$
$$K_0 = (P_0) \oplus (C_1 \oplus C_2)$$

This means that three known PT attacks can find the values of K_0, K_1 & K_2. But practically the block ciphers are not as simple as this one, they have more components and the S-boxes are not linear.

Scanned by CamScanner