Hello everyone and welcome to this

Module: Transposition Techniques,

Rail Fence, and Steganography, from

the unit: Concepts of Security and

Classical Encryption Techniques.

I am Ms. Sandra Fernandes from

St. Xavier's College.

In this session, we will be dealing

with one transposition technique

called the Rail Fence Technique,

and we shall see how we can convert

plain text to cipher text using this technique.

We will also understand a

little about Steganography,

which helps in concealing messages.

At the end of the session, you will be

able to understand and encrypt

plain text using Rail Fence technique.

You will also be able to explain

the features of steganography.

What is a transposition technique?

Transposition techniques perform some permutation over the plain text alphabets, wherein the order of the alphabets in the plain text is rearranged to form a cipher text. We shall consider the rail fence technique as an example of transposition technique and see how it can be used to encrypt data. This technique involves writing the plain text as a sequence of diagonals and then reading it, row by row, to produce the cipher text. Let us consider the plain text NETWORK SECURITY. In the first step, we shall write down the plain text as a sequence of diagonals. In the next step, we have to read the characters as a sequence of rows. So the first row would comprise of the characters NTOKEUIY.

This will be followed by EWRSCRT,

the characters from the second row.

This will give us the

cipher text for the

plain text NETWORK SECURITY.

The Rail Fence technique is very

easy to decrypt.

A plain text message can be hidden in

one of the two ways:

Using steganography - which conceals the

existence of the message and

Cryptography - which renders

the message unintelligible to outsiders,

by various transformations of the text.

So Steganography is the practice

of concealing a message within

another message or a physical object.

In fact, steganography has been

derived from the Greek word steganos,

which means covered or secret and

graphy, which means writing or drawing.

So steganography literally means

covered writing.

Let us see some of the classical

techniques with steganography:

arrangement of words or letters

within a text, spells out the real message.

Example, the sequence of the first

letters of each word, of the overall

message, gives out the hidden message.

Take for example, the statement

given in the slide -

NEVER EVER THROW WATER ON REAL KITTENS.

If we consider the first character

of each word, we get NETWORK,

which basically means NETWORK

is hidden in this message.

The second technique - character marking.

Selected letters of printed or typewritten

text are overwritten in pencil.

The marks are not visible unless the

paper is held at an angle to bright light.

Invisible ink.

A number of substances can

be used for writing,

but in this case, they leave no

visible trace until some chemical

or heat is applied to the paper.

Pin punctures.

Small pin punctures on selected

letters are normally not visible

unless the paper is held up in

front of a light.

Typewriter correction ribbon.

Used between

lines typed with a black ribbon.

The results of typing with the

correction tape are visible

only under a strong light.

Modern techniques make use of the least

significant bits of frames on a CD.

Kodak Photo CD formats

maximum resolution is 2048 X 3072 pixels.

Each pixel contains 24 bits

of RGB color information.

The least significant bits of each 24

bit pixel can be changed, without greatly

affecting the quality of the image.

So in this manner, you can hide a 2.3 megabyte

message in a single digital snapshot.

So let us once again define steganography.

Steganography is the art and science of

embedding secret messages in a cover

message in such a way, that no one, apart

from the sender and the intended recipient

suspects the existence of the message.

We will now look into two aspects of steganography:

Text steganography and Image steganography.

When information is hidden inside text files,

we call it text steganography.

It involves things like changing

the format of the existing text,

changing words within a text,

generating random character sequences,

or using context-free grammars

to generate readable text.

Images steganography,

on the other hand,

involves hiding the data by taking

the cover object as the image.

This is widely used cover source because

there are huge number of bits present in

the digital representation of an image.

Some applications of steganography.

Confidential communication

and secret data storing.

Steganography provides us with the

capability of hiding confidential data.

Also,

since the data is embedded,

there is no way to detect the

presence of hidden data.

Protection of data alteration.

Since the data is hidden,

the data will not be tampered

or altered by anyone.

Many modern printers make

use of steganography.

Tiny yellow dots are added to each page.

These dots are barely

visible and contain the encoded

printer serial numbers as well

as the date and the time stamp.

Steganography can also be used

for digital watermarking wherein,

a message can be hidden in an image,

in order to track and verify its source.

Limitations of steganography.

Steganography requires a lot of overhead

to hide relatively few bits of information.

Also, once the system is discovered,

it becomes virtually worthless.

This problem can be overcome, if the insertion

method depends on some sort of key.

Alternatively, a message can

be first encrypted and then

hidden using steganography.

To conclude, in this session, we

have seen how we can encrypt data

using the Rail Fence technique,

and we've also had a brief understanding

of how messages are concealed in

other objects using steganography.

Thank you.