Hello everyone and welcome to this

module on Encryption Techniques

from the unit Concepts of

Security and Classical Encryption.

I am Ms. Sandra Fernandes

from St. Xavier's College.

During the session, we will be considering

a few substitution techniques to

convert plain text to cipher text.

These would include Caesar Cipher,

Monoalphabetic technique

and the Polyalphabetic technique.

At the end of the session, you will

be able to understand the operation

of simple substitution techniques

to convert plain text to cipher text,

and you will also be able to

encrypt the plain text data

using Caesar cipher,

Mono-alphabetic cipher, and Vigenére Cipher.

Before we begin, let us define a few terms.

Cryptography is the art and science

of achieving security by encoding

messages to make them non-readable.

Cryptanalysis is a technique

of decoding messages from a non-

readable format back to a readable

format, without knowing how they were

initially converted from readable

format to non-readable format.

In other words,

it is nothing but, breaking a code.

Cryptology is a combination of

both cryptography and cryptanalysis.

A person who attempts to break a

cipher text message to obtain the

original plain text message is a Cryptanalyst.

An attack on the cipher text message,

wherein, the attacker attempts to

use all possible permutations and

combination is a Brute Force Attack.

So what is Plain Text and Cipher Text?

Any message, which is understood by

the sender, the recipient and also by

anyone else who gets access to that

message is considered as Plain Text

or we also can call it Clear Text.

In other words, a message which is

understandable and readable is Plain Text.

When a character is replaced by another one,

the process is called codification.

When a plain text message is

codified using any suitable scheme,

we get Cipher Text.

There are two methods to code

plain text to cipher text;

the Substitution technique and

the Transposition technique.

In substitution,

the characters of plain text message

are replaced by other characters,

numbers or symbols.

Let us see a few of substitution techniques,

starting with the Caesar cipher.

The Caesar cipher was

proposed by Julius Caesar,

and in this technique, an alphabet is

replaced with the one, three places down the line.

For example,

if we have the plain text

NETWORK SECURITY and we want to

encrypt this using Caesar cipher,

we will consider the first character N,

and three places down the line from N,

we have the character Q, which

will replace N.

Similarly,

H is 3 places after E.

T be replaced by W and

this process would continue.

This method is not very secure, in

the sense that, a cryptanalyst can

easily break into this and get the

original message by considering

the alphabets three places up.

A variation to this is the

modified version of Caesar cipher.

In this technique,

the cipher text alphabets can

be any places down the line.

Breaking the code is a little

difficult over here because we

have 25 possibilities to replace

any single character.

Suppose we have the cipher text

HYNQILE MYWOLCNS and we want to

find the original plain text,

we can create a table in this

manner, whereby we put all the

cipher text characters in the

row heading.

In the first row,

we start with the character, one place

down the line from the original character.

So H is followed by I, Y will

be followed by Z and so on.

In the 2nd row, we have characters

two places down the line and we can

create the entire table in this manner.

We will notice that in the 6th row we

have got the plain text NETWORK SECURITY.

Mono alphabetic cipher -

This makes use of substitution,

which is random, in the sense that,

each alphabet can be replaced

by any other random alphabet.

Here, each plain text character is

substituted by the same cipher text

character throughout the entire message.

We notice that the character E

will be replaced over here by the

character K in all occurrences of E.

The Homophonic substitution

cipher involves the substitution

of one plain text character with the

cipher text character at a time;

however, the cipher text character

can be any one of the chosen set.

So suppose we have the character

N and we want to replace it by

a character in the cipher text,

there is a chosen set.

Let us assume that the chosen set

is X, Y and Z, then N can be replaced

either by X, or by Y, or by Z.

In the Polygram substitution cipher,

there is a replacement of one entire block

of plain text with a block of cipher text.

So suppose we have the plain text

NETWORK and we have the cipher text HYNQILE,

replacing this entire block;

NET in the next block will have a

different set of characters replacing NET.

The next technique is the

Polyalphabetic cipher.

The Polyalphabetic cipher uses

multiple one character keys.

Each key encrypts one plain text character.

The first key encrypts the

first plain text character.

The second key encrypts the second plain text

character.

After all the keys are used,

they are recycled.

As an example,

let us consider the Vigenére Cipher.

The Vigenére Cipher uses a 26 X 26 table,

and it has a row heading and a

column heading, comprising of the

alphabets A to Z in the row heading,

as well as in the column heading.

The first row of the Vigenére Cipher table,

comprises of the alphabets, A to Z.

In the 2nd row,

we begin with the Alphabet B,

an end with Z and A,

in the last two columns.

The 3rd row starts with the character

C and ends with the alphabets

Z, A, B in the last three columns.

So we will notice that,

in this particular table,

every subsequent row from

the 2nd row onwards,

there will be a left shift of one character.

Let us now consider the plain text

NETWORK SECURITY and using the

key CODE we will encrypt this

plain text, using the Vigenére Cipher.

For this,

we will consider N, the first

character of the plain text in

the left-hand column heading

and C in the top row heading.

The intersection of these two

will give us the cipher text

associated with N, so that is P.

Before this, we need to

make sure that the length of the key

is equal to the length of the plain text.

So a key which repeats itself

is to be considered.

So in this case, N will be associated with

C, E will be associated with the

key O, T with D and W with E.

O will back again be associated

with C, R with O, K with D and S with E.

This will continue for the

entire plain text characters.

So now let us see the intersection.

The plain text alphabet N,

intersects with the plain text alphabet

C at P. So P becomes the

cipher text for N.

Similarly E will be intersecting with

O and the point of intersection will be S.

In this manner, we can find all

the ciphers with regards to each of

the characters of the plain text.

So to conclude, in this session, we have

seen a few substitution techniques

and we also know how we can encrypt

plain text data and convert

to cipher text using Caesar cipher,

Monoalphabetic cipher and

Polyalphabetic cipher.

As an example, we have taken Vigenére Cipher

under the Polyalphabetic cipher.

Thank you.