Hello everyone and welcome to this module

on Playfair Cipher and Vernam Cipher

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 two techniques to

convert plain text to cipher text;

the Playfair and Vernam cipher.

At the end of the session, you

will be able to understand the

operation of simple techniques to

convert plain text to cipher text,

and you will be able to encrypt

text using the two techniques

Playfair and Vernam cipher.

Let us start with the Playfair Cipher.

The Playfair Cipher has two main processes;

one is the creation and

population of a 5 X 5 matrix,

which is used to store a keyword,

which is nothing but a key, that is

used for encryption and decryption.

The second step involves

the encryption process.

Let us consider the creation

and population of the matrix.

There are certain rules that need to be

followed when we are creating the matrix.

We need to enter the keyword in the matrix

row-wise, left to right and then top to bottom.

Let us consider the keyword CODEWORD and

let us fill this into the Playfair Square.

We have to take into consideration,

that duplicates should not be

used in the Playfair Square.

So starting with the character

C of the keyword,

we will insert this in the first row, first column.

Similarly, O will be in the first row, second column;

D will be in the first row, third column;

E in the first row, fourth column;

W in the first row, fifth column.

The next character O will not

be used, since O has already

appeared in the first row, second column.

The character R will appear

in the second row, first column.

D again will not be appearing, since it

has already been listed in the first row.

Once we have finished inserting

all the characters of the keyword,

we fill the remaining spaces with

the alphabet starting from A to Z,

but also ensuring that

duplicates are not inserted.

We also have to note that I and J

use the same cell in the table.

So R will be followed by A, B.

C, D and E have already been listed in the first row.

F, G, H.

I and J occupy the same cell;

K, L, M, N.

O has already been listed in the

first row.

P, Q.

R is already listed.

S, T, U, V.

W is already there in the first row.

X, Y, Z.

This completes our Play Fair Square.

The second process, that is the

encryption process.

Let us consider

the plain text HELLO PARTICIPANT.

In this process - the first step, we

create groups of two characters in each

group with regards to the plain text.

So the first group will

contain the characters HE.

We have to keep in mind that,

if at all the group contains,

characters which are of similar type,

then we cannot use the second

character in the same group,

but instead it is replaced

with the character X.

The second character becomes

part of the next group.

It is also to be noted that, if at all the

last group contains only one character,

we need to add an X to that last group.

So in this manner,

let us create the various groups with regards

to the plain text HELLO PARTICIPANT.

So HE will form the first group.

LX will form the second group.

LO third group.

This will be followed by PA, RT, IC, IP, AN and

now we have only one character left,

so we will add an X to it

to form the last group.

In order to find the cipher text

with regards to this plain text,

we first define a rectangle with regards

to the elements of the first group.

H belongs to row 3 and column 1

with regards to the Playfair Square.

E, on the other hand,

belongs to row 1, column 4.

So we will now define a rectangle, which

will enclose both these characters.

So H will be at one end of the rectangle,

E will be at the other end of the rectangle.

In order to find the

cipher associated with H,

we have to look at the exact

opposite end in the same row

with regards to the character.

So H will be replaced by the character L,

whereas E will be replaced

by the character C.

So this gives us the two characters

LC which are substituted for the

plain text HE.

In a similar manner,

we can find the characters to be substituted

for the plain text characters L and X.

So after defining the rectangle,

we find that L will be replaced by K

and X will be replaced by Y,

Similarly, we can find

the characters for LO.

In the case of PA, we notice that

both, P and A belong to the same column.

In such a case, we will replace the

characters with the character immediately

following the plain text character.

So in other words, P will be replaced

by V and A will be replaced by I.

If at all, the character was

in the last row, then there is a

wrap around and the character will

be replaced by the character in

the first row in the same column.

That is, V will be replaced by the character O.

The same applies in the case of a row.

Lets say that the two characters in

a group were A and G.

A will be replaced by

the character immediately following it;

so in other words A will be replaced by B

and G will wrap around to the first

column in the second row, that is R.

So PA will have VI.

Similarly, RT will be replaced by GN.

In this manner, we can find the

cipher text associated with the

plain text HELLO PARTICIPANT.

Let us look at the rules once again.

The plain text message is

broken down into groups of two alphabets.

If both the alphabets are the same,

add an X after the first alphabet.

Also, if there is only one alphabet left

in the last group, add an X to it.

If both the alphabets in the pair

appear in the same row of the matrix,

replace them with alphabets

to their immediate right.

If the original pair is on

the right side of the row,

then wrap around to the left side of the row.

If both the alphabets in the pair,

appear in the same column of the matrix,

replace them with alphabets

immediately below them.

If the original pair is on

the bottom side of the row,

then wrap around to the top of the room.

If the alphabets are not in

the same row or column,

replace them with alphabets

in the same row respectively,

but at the other pair of corners of the

rectangle defined by the original pair.

The second technique,

Vernam Cipher is implemented using

a random set of non-repeating

characters as the input cipher text.

The input cipher text is never

used again for any other message,

and hence this technique is

also called one-time pad.

In this mechanism,

we assign a number to each plain text

character in increasing sequence.

That is,

A will be represented by

the number 0, B with 1,

Z will be represented by 25.

Every character of the input plain text will

thus be represented by its respective number.

Every character of the input cipher text,

which is also the one-time pad,

should also be represented

by its respective number.

Add each plain text character

number to the corresponding input

cipher text character number.

If the sum obtained is greater than 25,

we need to subtract 26 from it,

and finally translate each of

the numbers obtained back to

the corresponding alphabet,

giving us the cipher text.

Let us consider an example, HELLO

as the plain text and a one-time

pad given by the characters CLDXS.

We have the binary representations

of each of the characters of the

plain text and the one-time pad.

We will now consider the addition

of the binary representations.

H is represented by 7 and C represented

by 2 are added together to give us 9.

Similarly, E represented by 4 and L

represented by 11 are added to give us 15.

This process is continued for all the

characters of the plain text as well as the

one-time pad.

We now look at the

output and check to see, which of

these numbers is greater than 25.

We find that the last two numbers

have a value of 34 and 32 and so we need

to subtract 26 from these two numbers,

to give us the final result which

comprises of the representation 9, 15, 14, 8 and 6.

This is back again

converted to its alphabetic

representation to give us the cipher text

JPOIG for the plain text HELLO.

So to conclude, in this module we

have learned two techniques and

seen how we can encrypt data using

Playfair Cipher and Vernam Cipher.

Thank you.