Hello everyone and welcome to this module:

Algorithm Types and Modes, Block

Cipher Operation, Electronic Code Book,

Cipher Block Chaining and Block

Cipher Principles,

from the unit:

Symmetric and Asymmetric Key Algorithms.

I am Sandra Fernandes

from St. Xavier's College.

In this session, we will understand

the difference between Stream

ciphers and Block ciphers.

We will also consider two algorithm modes,

Electronic Code Book and

Cipher Block Chaining.

And final, we will elaborate

on some block cipher principles.

At the end of the session, you will

be able to understand the difference

between stream ciphers and block ciphers.

You will also be able to describe

ECB and the CBC mode of operation,

and finally explain the block

cipher principles.

Before we understand computer

based cryptographic algorithms,

let us focus on two key aspects

of such algorithms;

the algorithm type and the algorithm mode.

An algorithm type defines what

size of plain text should be encrypted

in each step of the algorithm,

whereas the algorithm mode defines

the details of the cryptographic

algorithm, once the type is decided.

Cipher text can be generated

from plain text in two ways:

Stream ciphers, which involves byte

by byte encryption and decryption

and Block ciphers which is block

by block encryption and decryption.

Let us start with stream ciphers.

Stream cipher technique involves

the encryption and decryption

of one plain text byte at a time.

Let us consider the plain text SECURITY,

and we shall assume that 01011100

is the binary equivalent of this.

Let us also consider the binary equivalent

of a key and assume it to be 10010101.

Applying the XOR logic for

converting it into cipher text,

we all know that, the output of an XOR will

be 1, only if both inputs are different.

That is, one is a 0 and the other is a 1.

So after applying the XOR,

we get 11001001, which

will give us the cipher text.

There is a very interesting property of

XOR, that is, when it is used twice,

it produces the original data.

Let us assume the binary

representation of A is 101.

B is 110.

If we perform the XOR of A and B,

we get 011 which is denoted as C.

Let us consider C,

with its binary representation

011 and A represented by 101.

If we apply an XOR to C and A,

we get 110 which is nothing but B.

Similarly, if we consider C: 011 and B: 110,

after the XOR operation, we get A.

Block ciphers involve the encryption and

decryption of one block of text at a time.

Let us consider the plain text,

TWO_AND_TWO.

The first block would contain the word TWO,

the second block would have _AND_

the third block would have TWO.

After encryption,

we notice that the first and the third

block will have the same cipher text.

This is a problem because we have

repeating text patterns and in such a

case, the same cipher would be generated.

So this makes it easy for a cryptanalyst

to decrypt and get back the original data.

The solution:

Block ciphers

are used in chaining mode,

wherein the previous block of cipher

is mixed with the current block.

Block ciphers are much faster as

compared to stream ciphers because stream

ciphers work on one byte at a time.

Hence, block ciphers are

mostly used in algorithms.

The elements of a group are the

cipher text blocks with each possible key.

Grouping means, how many times the

Plain text is scrambled in various

ways to generate the cipher text.

What is confusion and diffusion?

Confusion, which is achieved

by means of substitution,

is a technique of ensuring that

the cipher text gives no clue

about the original plain text.

It spoils the attempts of a cryptanalyst

to look for patterns in the cipher text so

as to get the corresponding plain text.

Diffusion, on the other hand, is achieved

by using transposition techniques.

It increases the redundancy of

the plain text by spreading it

across rows and columns.

Stream ciphers rely only on confusion,

whereas block ciphers use

both, confusion and diffusion.

Algorithm mode is a combination of a

series of the basic algorithm steps

on block ciphers and some kind of

feedback from the previous step.

There are four important modes:

Electronic Code Book ECB,

Cipher Block Chaining CBC,

Cipher Feedback CFB and

Output Feedback OFB

There is also a variation of

OFB called as counter CTR.

The first two modes ECB and CBC,

work on block ciphers,

whereas CFB and OFB work on block

ciphers acting as stream ciphers.

In this session, we will be

dealing with ECB and CBC.

In the case of the Electronic Code Book,

the incoming plain text message is

divided into blocks of 64 bits each.

Each block is then encrypted

Independently, using the same key,

for the purpose of encryption.

So looking at the diagram,

we have the plain text Block 1,

which is encrypted using a key,

to give us the first cipher text block.

The 2nd block in Step 2, will be

considered and encrypted using the same key

and we get the cipher text Block 2.

This will continue for all

the plain text blocks.

At the receiver's end, the incoming

data is divided into 64 bit blocks.

Using the same key that

was used for encryption,

each block is decrypted to give

the corresponding plain text block.

Since the single key is used for

encrypting all the blocks of a message,

if a plain text block repeats

in the original message,

the corresponding cipher text block will

also repeat in the encrypted message.

Hence, this technique is used

only for short messages.

In the diagram, we have the cipher text

Block 1, decrypted using the same key

to give us the plain text Block 1.

In Step 2, we consider the cipher text

block to again decrypt it with the same

key to give us the plain text Block 2.

This process continues for all

the cipher text blocks.

Cipher Block Chaining.

Cipher block chaining ensures that even if

a block of plain text repeats in the input,

these identical plain text blocks, give totally

different cipher text blocks in the output.

This is achieved using a feedback

mechanism to the block cipher.

The results of the encryption of the

previous block are fed back into

the encryption of the current block.

Each block is used to modify the

encryption of the next block.

Each block of cipher text is dependent on the

corresponding current input plain text block,

as well as all the previous plain text blocks.

Let us first consider the encryption process.

In the first step, we have two inputs:

the plain text Block 1 and a random block

of text called the Initialization Vector.

The Initialization Vector

is randomly generated

and is unique for every block.

The initialization vector is XORed

with the plain text Block 1,

the output of which is encrypted using a key,

to give us the cipher text Block 1.

This becomes the feedback

to the next plain text block.

In the second step,

the second text block, that is, the

plain text Block 2 is XORed with the

cipher text block from the previous step.

The output is then encrypted

with the same key to give

us the cipher text Block 2.

This process continues for

all the blocks of plain text.

In the decryption phase,

in Step 1, the cipher text Block 1

is decrypted using the key.

The output is then XORed with

the initialization vector

to give us the plain text Block 1.

In Step 2, the cipher text block

will be used as a feedback to

generate the plain text Block 2.

So in step 2, we will consider

the cipher text Block 2 and

decrypt it using the same key.

This is then XORed with the cipher text Block 1,

that is, the cipher text block

of the previous step, to give

us the plain text Block 2.

This process will continue for all the

n blocks of cipher text.

Let us look at some of the Block

Cipher Principles.

Block Size.

A larger block size means greater security,

but reduced encryption/decryption

speed for a given algorithm.

The greatest security is achieved

by greater diffusion.

Traditionally, 64 bits bit blocks are widely considered.

Key size.

Larger key size means

greater security, but may decrease

the encryption and decryption speed.

The greater security is achieved by

greater resistance to brute force

attacks and greater confusion.

Key sizes of 128 bits has become

a common size.

Number of rounds.

Multiple rounds offer increasing security.

A typical size is 16 rounds.

Subkey generation algorithm.

Greater complexity in this algorithm should

lead to greater difficulty of cryptanalysis.

Round function F

Greater complexity means

greater resistance to cryptanalysis.

So to conclude,

in this session, we have seen the

two algorithm modes,

Electronic Code Block and Cipher

Block Chaining.

We have also elaborated on the various

principles related to block cipher.

Thank you.