בס"ד

Block Ciphers review is an incryption method

Line of blocks that each contains the incryption code

Lets say a string

“I will go home”

`I` ` ` `w` `i` `l`

Each letter is a block

Each block contains a letter

In ECB:

Elctronic Code Block

Each letter is for itself

The thing about ECB is that it EACH BLOCK stands by itself

Now, If a hacker hacked the first block, He has the lets say “plain text” of the first block

\*\*The hacker gets Enough information with 1 block alone mostly\*\*

Each Block / Letter contains 64Bit

In CBC:

Cypher Block Chain:

In CBC despite ECB, Contains a chain for all blocks

Which means that if an hacker hacked the first block, He needs the second, the third and so on blocks To Have ANY kind of information!

Because each blocks needs the block after and before him,

So in this method If you want any information, Even a bit of, you need ALL the blocks in the chain.

===========================================================================

Block ciphers examples

AES

IDEA

Twofish

Blowfish

DES

[REGENDEL]

The AES is the next generation of the old DES

Inside AES contains a s REGENDEL

AES

Symmetric cipher vs Asymteric

Symmetric is one key, asymetric 2

Symetric is two functions one key

Asymetric is 2keys PER pc,

One for private, One for public

To have a connection between 2 pcs, You need total 4 keys, 2 for each.

One Symmetric format is :

Each pc can transmit to another one With one key,

If one’s pc wants to communicate to another, He will speak with another key

Which means that if he dosent have the private key of lets say ofek and yanai’s pcs he cant speak with them

That sums up to each pc has it own key, in a class of 30 pcs you will need 30 Keys!

And to talk to another pc you need his private key.

The disatvantage to that is you need to manage 30 keys !

Another format is that the whole class has only 1key!

Means: That one’s pc in the class can communicate with another Without the need of another-one’s key.

Less complicated, but also less security.