Bellevue University

Electronic Code Book

And

Cipher Block Chaining

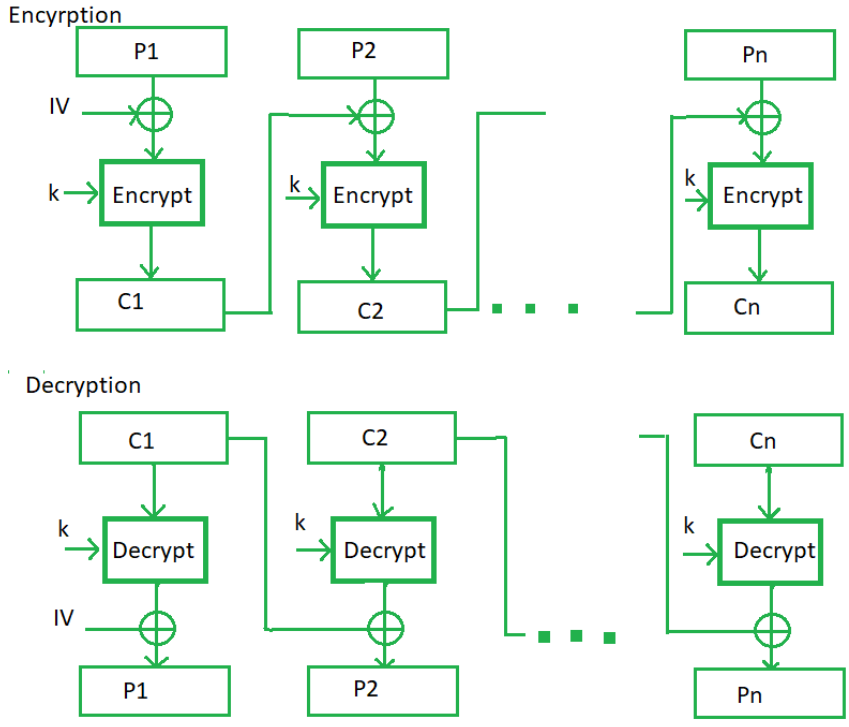
Timothy Jelinek

CIS313-T301 Cryptography

9/17/2023

The electronic code book is known for being the easiest block cipher mode of functioning. It is known to be the easiest because it uses direct encryption of every block of input plaintext and output is in the form of blocks of ciphertext that are encrypted. According to GeeksForGeeks (2023) “generally, if a communication is larger than *b* bits in size, it can be broken down into a bunch of blocks and the procedure is repeated.” (p1). There are a couple of advantages of using the electronic code book which include the possibility of parallel encryption of blocks of bits which makes encryption brisk and it’s a simple way of using the block cipher. A disadvantage of using the electronic code book is that since it has a direct relationship between plaintext and cipher text, it is prone to cryptanalysis.

Attached is an image of the process from GeeksForGeeks.



Cipher block chaining is the advancement made of the electronic code book because it didn't meet all the security requirements. Some advantages of using cipher block chaining are that it works well when the input bits are greater than *b*, cipher block chaining is a good authentication mechanism, and it is more resistant towards cryptanalysis than the electronic code book. The disadvantage is that it can't do parallel encryption like the electronic code book. This is a good example of choosing which is more secure or which is quicker for the job.

Sources:

"Block Cipher modes of Operation." Meghna, geeksforgeeks.org, https://www.geeksforgeeks.org/block-cipher-modes-of-operation/#. Accessed 17 September 2023.