2021201041
Nvss Maneesh Gupta

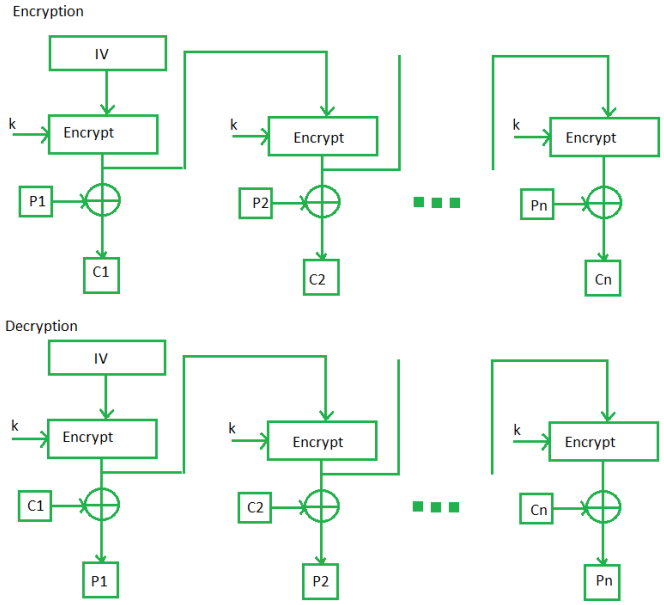
CPA Security – Output Feedback Mode

Using PRF alone will make a deterministic encryption which is prone to CPA attacks. To make an encryption CPA secure we need probabilistic encryption. There are multiple ways to obtain this. The following is one such approach

1. Simply generating random noise r, key k of length equal to length of plain text i.e. $r, k \in \{0,1\}^n \; where \; n \; is \; the \; length \; of \; plain \; text.$
2. Encrypt r with a key k using PRF $F_k(r)$
3. XOR encrypted r with plain text $F_k(r) \oplus m, m \; is \; plain \; text.$
4. Send the cipher text $c := < r, F_k(r) \oplus m >$
5. At the receiver end, on input k and cipher text $c =< r, s >$ plain text $m := F_k(r) \oplus s$

The above implementation will generate an output cipher text of double the length of the plain text.

To obtain probabilistic encryption without length doubling, we use one of the modes of operation. Output Feedback Mode is used here.



1. The plain text is divided blocks of equal size.
2. An initialization vector (IV) is encrypted using the pseudo random function and the key.
3. Both the key and IV are same length as of the block.
4. The encrypted IV is then used as IV for the next iteration.
5. Encrypted IV is XORed with a block of plain text to obtain a cipher text block.
6. Both the IV along with the concatenated cipher blocks are sent to receiver.

References

[1] J. K. a. Y. Lindell, Introduction to Modern Cryptography.

[2] B. Micali, "Hardcord bits," [Online]. Available: https://crypto.stanford.edu/pbc/notes/crypto/hardcore.html.

[3] Lecture Slides

[4] https://www.geeksforgeeks.org/block-cipher-modes-of-operation/