Modes Of Operation

Dipesh Pokhrel

April 12, 2022

Block Cipher break up Plain-text into blocks P_1, P_2, P_3..... encrypt blocks one at a time. *NOTE* Use the same key everytime.

1 How do we actually encrypt all the blocks to get cipher-text blocks C_1, C_2?

"Obvious" answer will be **Electronic Codebook (ECB)**.

$C_1 \rightarrow E_k * (P_1)$

$C_2 \rightarrow E_k * (P_2)$

$C_3 \rightarrow E_k * (P_3)$

This is how the hill cipher worked. $E_k(P) \rightarrow S(P \oplus k)$

1.1 Problem

It preserves patterns in the plain-text.

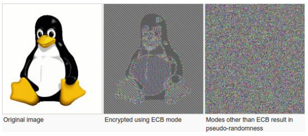

Figure 1:

2 Cipher Block Chain

Also known as **CBC**

Use the cipher-texts to scramble the plain-text before encryption.

Choose a random initial block called IV $= C_0$

Send this unencrypted in "cleartext"

2.1 To get more cipher-text blocks we use,

See the figure below:

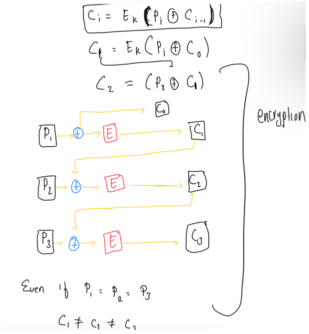

Figure 2:

2.2 Decryption. How would Bob recover the plain-texts from $C_0, C_1, C_2, C_3 \ldots$.

$P_1 \oplus C_0 \rightarrow D(C_1)$

$P_1 \rightarrow D(C_1) \oplus C_0$

In General, $P_i \rightarrow D_k(C_i) \oplus C_{i-1}$

3 Cipher Feedback (CFB)

- Works as a stream cipher start with $IV = C_0$

$\boxed{C_i \rightarrow E_k(C_{i-1}) \oplus P_i}$ (Random Number Generator)

3.1 Decryption

$\boxed{P_i \rightarrow E_k(C_{i-1}) + C_i}$

Never use the decryption function

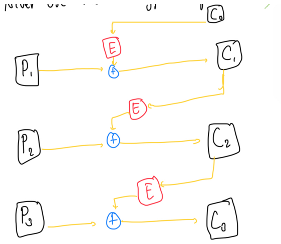

Figure 3:

4 Output Feedback (OFB)

Starts with IV $\rightarrow O_0$

$O_i \rightarrow E_k(O_{i-1})$ This is the output blocks

$C_i \rightarrow P_i \oplus O_i$

4.1 Advantages

All of the output blocks can be precomputed before knowing the plain-texts.

4.2 Decryption

$P_i \rightarrow C_i \oplus O_i$

** Like One time pad where O_i is the **key**

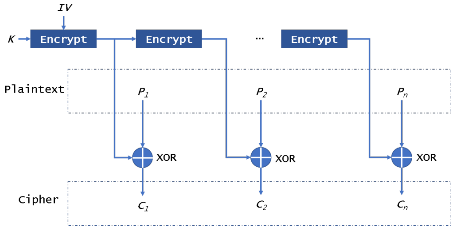

Figure 4:

5 Counter (CTR)

Start with IV $= X_0$
$X_i \rightarrow \underline{X_{i-1} + 1}$(increment by 1)

$$C_i \rightarrow P_i \oplus E_k(X_i) \rightarrow Ciphertext$$

In practice right now must websites uses GCM Galois Counter Mode. This is Counter (CTR) + "Authentication"

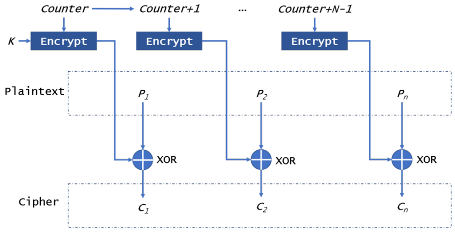

Figure 5:

REFRENCES