Les modes d'utilisation

1 Le mode Electronic Code Book (ECB)

Chiffrement :

Entrée : k blocs de texte clair de taille t_d, $P_1P_2\cdots P_k$.

Sortie : k blocs de chiffré de taille t_d, $C_1C_2\cdots C_k$.

$$
\begin{aligned}
&C_1 = \mathcal{E}_K(P_1)\\
&\ldots\\
&C_i = \mathcal{E}_K(P_i)\\
&\ldots\\
&C_k = \mathcal{E}_K(P_k)
\end{aligned}
$$

Déchiffrement :

Entrée : k blocs de chiffré de taille t_d, $C_1C_2\cdots C_k$.

Sortie : k blocs de texte clair de taille t_d, $P_1P_2\cdots P_k$.

$$
\begin{aligned}
&P_1 = \mathcal{D}_K(C_1)\\
&\ldots\\
&P_i = \mathcal{D}_K(C_i)\\
&\ldots\\
&P_k = \mathcal{D}_K(C_k)
\end{aligned}
$$

2 Le mode Cipher FeedBack (CFB)

Chiffrement :

Entrée : k blocs de texte clair de taille $s < t_d$, $P_1P_2 \cdots P_k$.

Sortie : 1 blocs de chiffré de taille t_d suivi de k blocs de chiffré de taille s, $I_1C_1C_2 \cdots C_k$.

$$
\begin{aligned}
& I_1 \leftarrow \{0,1\}^{t_d} \\
& Z_1 = \mathcal{E}_K(I_1) \\
& C_1 = P_1 \oplus MSB_s(Z_1) \\
& \dots \\
& I_i = LSB_{t_d-s}(I_{i-1})||C_{i-1} \\
& Z_i = \mathcal{E}_K(I_i) \\
& C_i = P_i \oplus MSB_s(Z_i) \\
& \dots \\
& I_k = LSB_{t_d-s}(I_{k-1})||C_{k-1} \\
& Z_k = \mathcal{E}_K(I_k) \\
& C_k = P_k \oplus MSB_s(Z_k)
\end{aligned}
$$

Déchiffrement :

Entrée : 1 blocs de chiffré de taille t_d suivi de k blocs de chiffré de taille s, $I_1C_1C_2 \cdots C_k$.

Sortie : k blocs de texte clair de taille $s < t_d$, $P_1P_2 \cdots P_k$.

$$
\begin{aligned}
& Z_1 = \mathcal{E}_K(I_1) \\
& P_1 = C_1 \oplus MSB_s(Z_1) \\
& \dots \\
& I_i = LSB_{t_d-s}(I_{i-1})||C_{i-1} \\
& Z_i = \mathcal{E}_K(I_i) \\
& P_i = C_i \oplus MSB_s(Z_i) \\
& \dots \\
& I_k = LSB_{t_d-s}(I_{k-1})||C_{k-1} \\
& Z_k = \mathcal{E}_K(I_k) \\
& P_k = C_k \oplus MSB_s(Z_k)
\end{aligned}
$$

3 Le mode Cipher Block Chaining (CBC)

Chiffrement :
Entrée : k blocs de texte clair de taille t_d, $P_1 P_2 \cdots P_k$.
Sortie : $k+1$ blocs de chiffré de taille t_d, $C_0 C_1 C_2 \cdots C_k$.
.

$$C_0 \leftarrow \{0,1\}^{t_d}$$
$$C_1 = \mathcal{E}_K(C_0 \oplus P_1)$$
$$\ldots$$
$$C_i = \mathcal{E}_K(C_{i-1} \oplus P_i)$$
$$\ldots$$
$$C_k = \mathcal{E}_K(C_{k-1} \oplus P_k)$$

Déchiffrement :
Entrée : $k+1$ blocs de chiffré de taille t_d, $C_0 C_1 C_2 \cdots C_k$.
Sortie : k blocs de texte clair de taille t_d, $P_1 P_2 \cdots P_k$.

$$P_1 = \mathcal{D}_K(C_1) \oplus C_0$$
$$\ldots$$
$$P_i = \mathcal{D}_K(C_i) \oplus C_{i-1}$$
$$\ldots$$
$$P_k = \mathcal{D}_K(C_k) \oplus C_{k-1}$$

4 Le mode Output FeedBack (OFB)

Chiffrement :
Entrée : k blocs de texte clair de taille t_d, $P_1P_2\cdots P_k$.
Sortie : $k+1$ blocs de chiffré de taille t_d, $Z_0C_1C_2\cdots C_k$.
.

$$
\begin{aligned}
&Z_0 \leftarrow \{0,1\}^{t_d}\\
&Z_1 = \mathcal{E}_K(Z_0)\\
&C_1 = Z_1 \oplus P_1\\
&\ldots\\
&Z_i = \mathcal{E}_K(Z_{i-1})\\
&C_i = Z_i \oplus P_i\\
&\ldots\\
&Z_k = \mathcal{E}_K(Z_{k-1})\\
&C_k = Z_k \oplus P_k
\end{aligned}
$$

Déchiffrement :
Entrée : $k+1$ blocs de chiffré de taille t_d, $Z_0C_1C_2\cdots C_k$.
Sortie : k blocs de texte clair de taille t_d, $P_1P_2\cdots P_k$.

$$
\begin{aligned}
&Z_1 = \mathcal{E}_K(Z_0)\\
&P_1 = Z_1 \oplus C_1\\
&\ldots\\
&Z_i = \mathcal{E}_K(Z_{i-1})\\
&P_i = Z_i \oplus C_i\\
&\ldots\\
&Z_k = \mathcal{E}_K(Z_{k-1})\\
&P_k = Z_k \oplus C_k
\end{aligned}
$$

5 Le mode Counter (CTR)

Chiffrement :

Entrée : k blocs de texte clair de taille t_d, $P_1 P_2 \cdots P_k$.

Sortie : $k+1$ blocs de chiffré de taille t_d, $(CTR_1) C_1 C_2 \cdots C_k$.

.

$$CTR_1 \leftarrow \{0,1\}^{t_d}$$
$$Z_1 = \mathcal{E}_K(CTR_1)$$
$$C_1 = Z_1 \oplus P_1$$
$$\ldots$$
$$CTR_i = CTR_{i-1} + 1 \mod 2^{t_d}$$
$$Z_i = \mathcal{E}_K(CTR_i)$$
$$C_i = Z_i \oplus P_i$$
$$\ldots$$
$$CTR_k = CTR_{k-1} + 1 \mod 2^{t_d}$$
$$Z_k = \mathcal{E}_K(CTR_k)$$
$$C_k = Z_k \oplus P_k$$

Déchiffrement :

Entrée : $k+1$ blocs de chiffré de taille t_d, $(CTR_1) C_1 C_2 \cdots C_k$.

Sortie : k blocs de texte clair de taille t_d, $P_1 P_2 \cdots P_k$.

$$Z_1 = \mathcal{E}_K(CTR_1)$$
$$P_1 = Z_1 \oplus C_1$$
$$\ldots$$
$$CTR_i = CTR_{i-1} + 1 \mod 2^{t_d}$$
$$Z_i = \mathcal{E}_K(CTR_i)$$
$$P_i = Z_i \oplus C_i$$
$$\ldots$$
$$CTR_k = CTR_{k-1} + 1 \mod 2^{t_d}$$
$$Z_k = \mathcal{E}_K(CTR_k)$$
$$P_k = Z_k \oplus C_k$$