

Lecture 9: Modes of Operation

Modes of operation	Electronic CodeBook (ECB)	Cipher Block Chaining (CBC)	Cipher Feedback (CFB)	Output Feedback (OFB)	Counter (CTR)
Description	$C_i = E(K, P_i)$ $P_i = D(K, C_i)$	$C_i = E(K, C_{i-1} \oplus P_i)$ $P_i = C_{i-1} \oplus D(K, C_i)$ $C_0 = IV$ (initialization vector)	$S_s(X)$ is the most significant s bits of X ; $L_s(X)$ is the least significant s bits of X ; Shift register: R (64bits) C_i , and P_i are units of transmissions which have s bits; usually $s = 8$. $R_i = S_{64-s}(R_{i-1}) \parallel C_{i-1} \rightarrow 64$ bits $C_i = P_i \oplus S_s(E(K, R_i)) \rightarrow s$ bits $P_i = C_i \oplus S_s(E(K, R_i)) \rightarrow s$ bits $R_0 = IV$ Note that encryption algorithm is used in decryption procedure.	$S_s(X)$ is the most significant s bits of X ; $L_s(X)$ is the least significant s bits of X ; Shift register: R (64bits) O_i : encryption output O_i , C_i , and P_i are both s bits; usually $s = 8$. $R_i = S_{64-s}(R_{i-1}) \parallel O_{i-1} \rightarrow 64$ bits $O_i = S_s(E(K, R_i)) \rightarrow s$ bits $C_i = P_i \oplus O_i \rightarrow s$ bits $P_i = C_i \oplus O_i \rightarrow s$ bits $R_0 = IV$ Note that encryption algorithm is used in decryption procedure.	$O_i = E(K, Ctr+i-1)$ $C_i = P_i \oplus O_i$ $P_i = C_i \oplus O_i$
Confidentiality & Integrity protection	(1) Same plaintext blocks produce same ciphertext blocks. This means that the data pattern is revealed. For example, ECB mode will reveal the image pattern if used to encrypt image files. (2) Rearranging the blocks is undetectable.	(1) random IV gurantees that even if the same message is repeated, the ciphertext is different. (2) modifying ciphertext blocks and rearranging ciphertext blocks undetected are still possible.	No integrity protection; Better in detecting alterations than OFB	Able to make controlled changes to recovered plaintext. No integrity protection; not as well as CFB	Same as other modes
Error propagation	No	One block	64/s units of transmission.	No	No
Application	Block oriented transmission; Not suitable for long messages or highly structured messages. Good for single values (e.g. keys)	Block-oriented transmission; General-purpose encryption; message authentication code design	Stream-oriented transmission, which has the following benefit: (1) no need for padding;(2) ciphertext has the same length of message; (3) pipeline is possible for encryption, thus good for low-latency real-time transmission encryption.	Stream-oriented transmission; transmission over noisy channel; Able to preprocess to generate one-time pad	Block-oriented transmission; Able to preprocess to generate one-time pad; Random access; High performance requirement; IPsec