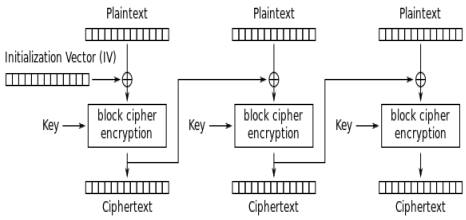
Block mode

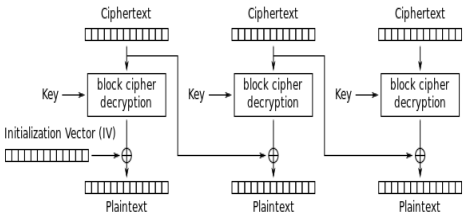
Cipher block chaining (CBC) [edit]

Ehrsam, Meyer, Smith and Tuchman invented the cipher block chaining (CBC) mode of operation in 1976.[23] In CBC mode, each block of plaintext is XORed with the previous ciphertext block before being encrypted. This way, each ciphertext block depends on all plaintext blocks processed up to that point. To make each message unique, an initialization vector must be used in the first block.

CBC	
Cipher block chaining	
Encryption parallelizable	No
Decryption parallelizable	Yes
Random read access	Yes



Cipher Block Chaining (CBC) mode encryption



Cipher Block Chaining (CBC) mode decryption

If the first block has index 1, the mathematical formula for CBC encryption is

$$C_i = E_K(P_i \oplus C_{i-1}),$$
$$C_0 = IV,$$

while the mathematical formula for CBC decryption is

$$P_i = D_K(C_i) \oplus C_{i-1},$$
$$C_0 = IV.$$

Padding:

The other is to append a byte with value 0x80 (a byte with value 1000 0000 in binary) followed by as many zero bytes as needed to fill the last block. This method is known as ISO padding, which is short for ISO/IEC 9797-1 padding method 2. The padding itself is bit-level padding, a single bit valued 1 is added, and then add 0 valued bits until you reach the block size.

As for how to know whether a message is padded, the answer is a message will *always* be padded: even if the last chunk of the message fits perfectly inside a block (i.e. the size of the message is a multiple of the block size), you will have to add a dummy last block.