possible zero padding

$$M = M_1 M_2 \cdots \overbrace{M_N}, \quad |M_i| = b.$$

ECB:

Encryption $C_j = E(k, M_j)$. $j = 1, \ldots, N$

Decryption $M_j = D(k, C_j)$. $j = 1, \ldots, N$.

If the same b-bit block of plaintext appears more than once in the message, say $M_i = M_j$.

It always produces the same ciphertext, say $C_i = C_j$.

Cipher Block Chaining Mode.

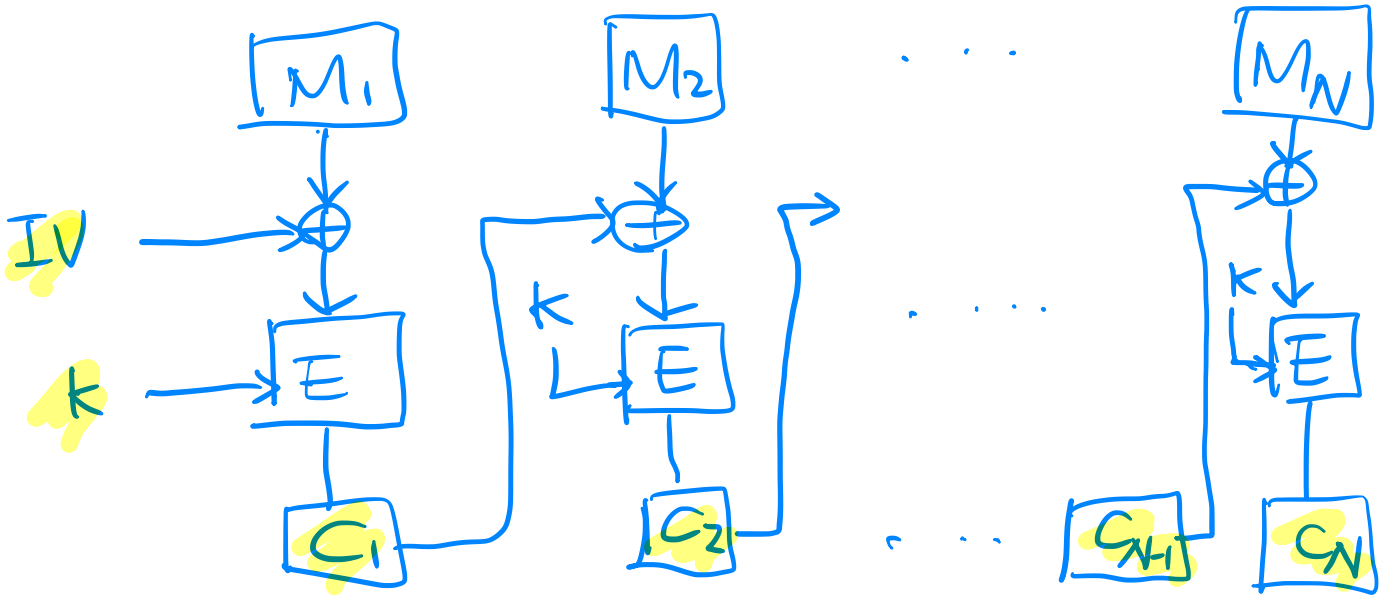
(If the same plaintext block is repeated, they are encrypted to different ciphertext blocks.).

$M = M_1 M_2 \cdots M_N$.

initialization vector.

$C_1 = E(k, IV \oplus M_1)$, where IV is a random vector.

$$C_j = E(k, C_{j-1} \oplus M_j)$$



Decryption

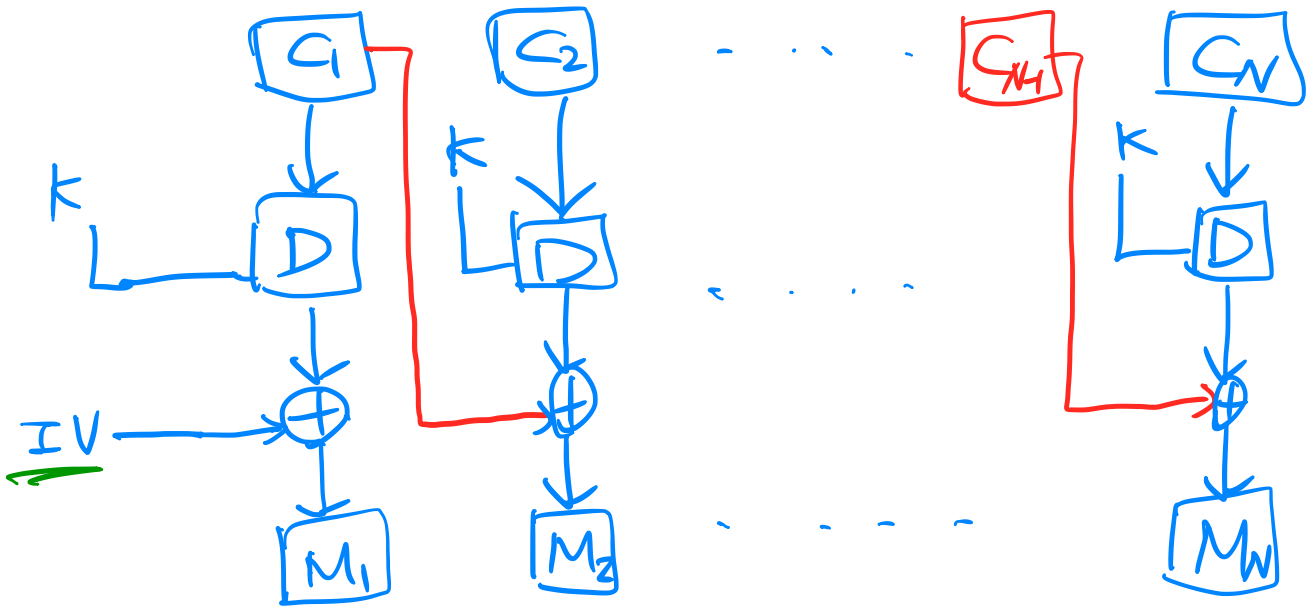
① $D(k, C_1) = IV \oplus M_1$

$\Rightarrow M_1 = IV \oplus D(k, C_1)$

② $D(k, C_j) = D(k, E(k, C_{j-1} \oplus M_j))$

$= C_{j-1} \oplus M_j$

$\Rightarrow M_j = C_{j-1} \oplus D(k, C_j)$



The IV must be known to both the sender & receiver but unpredicatable to the adversaries.

Send the IV to the receiver, using the ECB mode.

Let X[i] denote the ith bit of a string X.

$$M_1[i] = IV[i] \oplus D(k, C_1)[i]$$

$$M_1[i]' = IV[i]' \oplus D(k, C_1)[i]$$

where $X[i]' = X[i] \oplus 1$ (complement)

If an opponent is able to fool the receiver into using a different value of IV, then the opponent is able to invert selected bits in M_1.

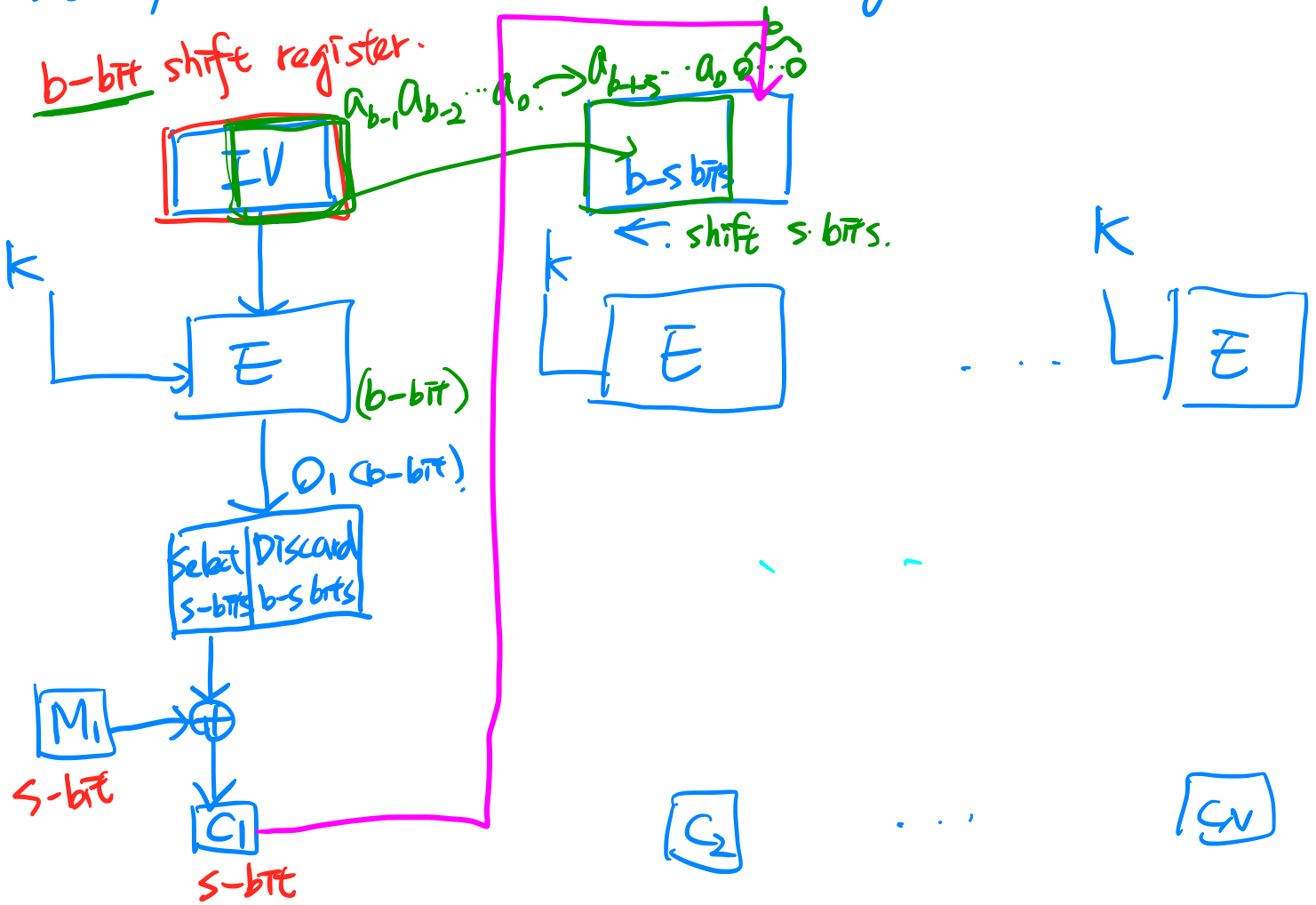
Cipher Feedback Mode

A stream cipher eliminates the need to pad a message to an integral number of blocks.

One desired property of a stream cipher is that the ciphertext is of the same length as the plaintext.

The unit of transmission s ($b = 64, 128$; $s = 8$.)

In this case rather than blocks of b bits, the plaintext is divided into segments of s bits.



C_j cannot be encrypted in parallel.