Modes of operation for block ciphers

Block cipher with n-bit blocks, e.g. DES: $n = 64$, AES: $n = 128$

Message m split into blocks of n bits, i.e.,

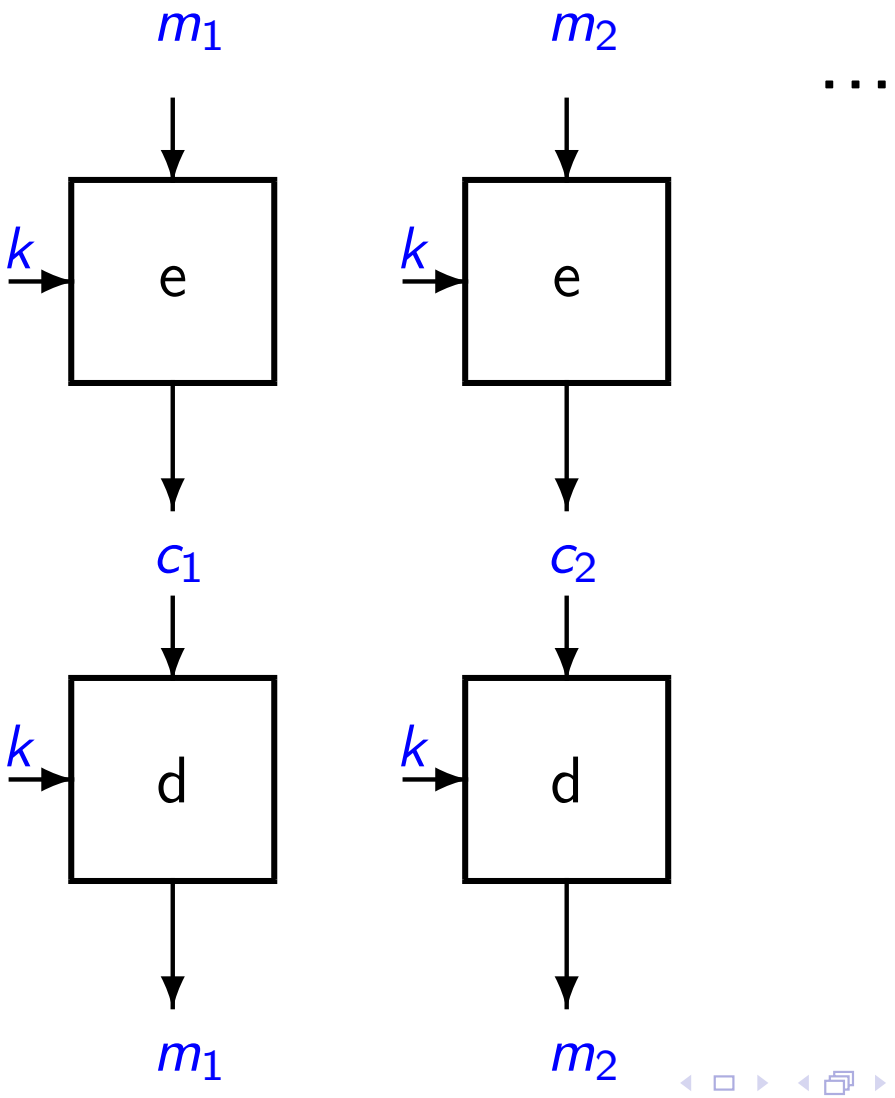
$$m = m_1, m_2, ..., m_t,$$

where $|m_i| = n$

Many modes of operation: ECB (dangerous, don't use), CBC, CFB, OFB, CTR, GCM...

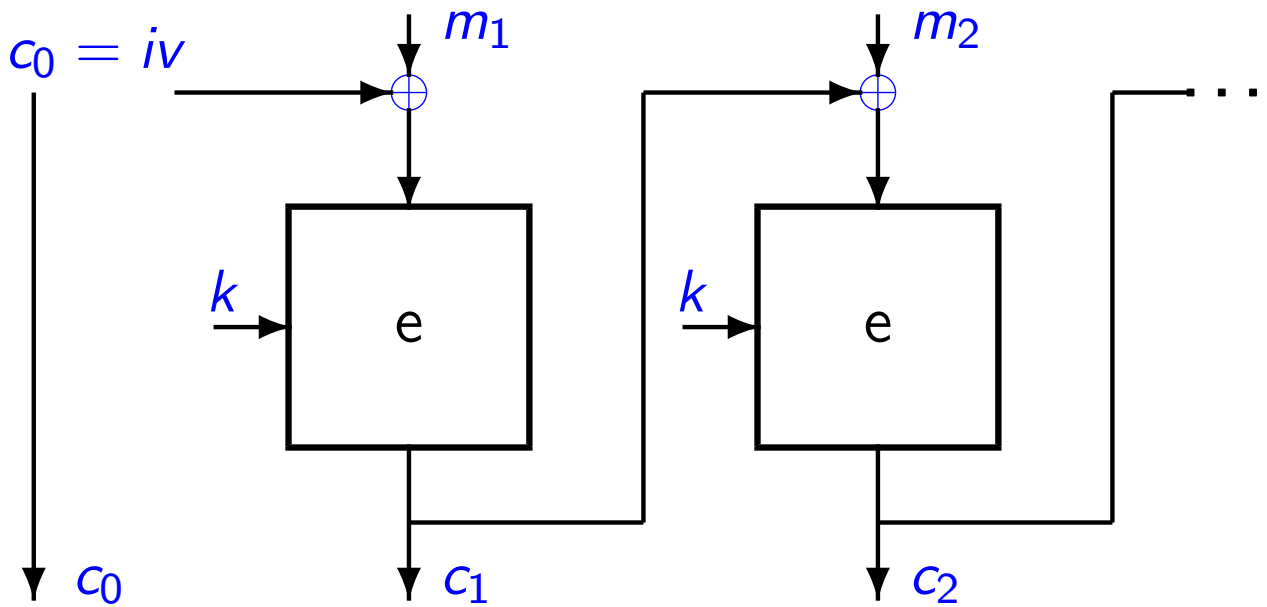
ECB mode (dangerous, don't use)

Encryption and decryption



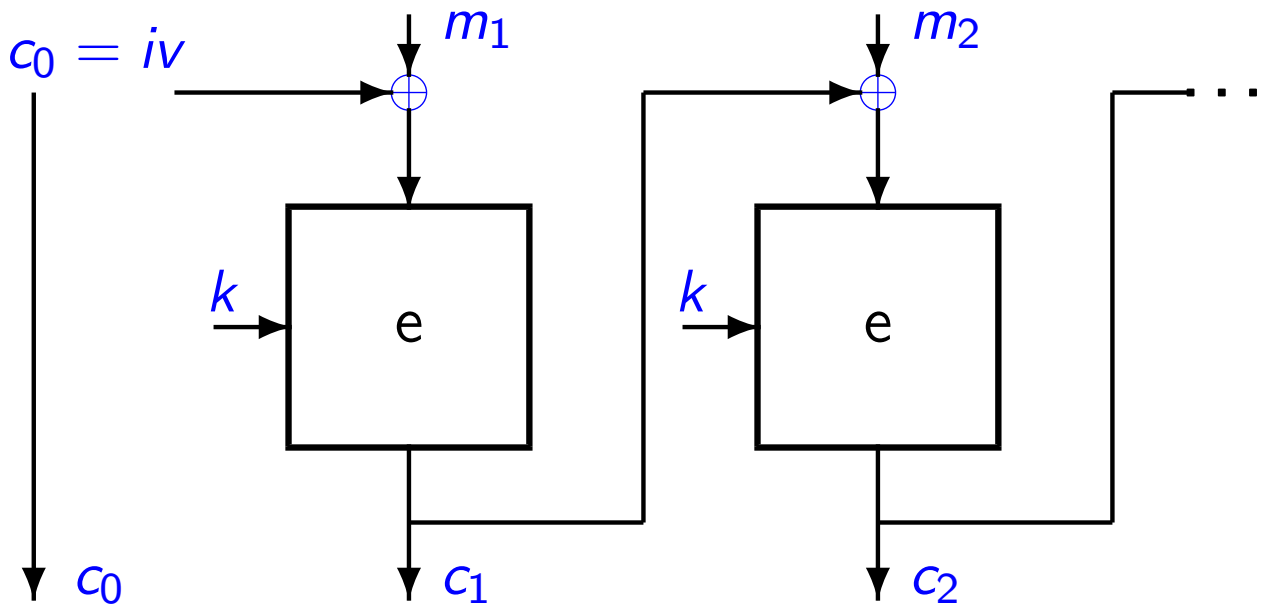
CBC mode

Encryption



CBC mode

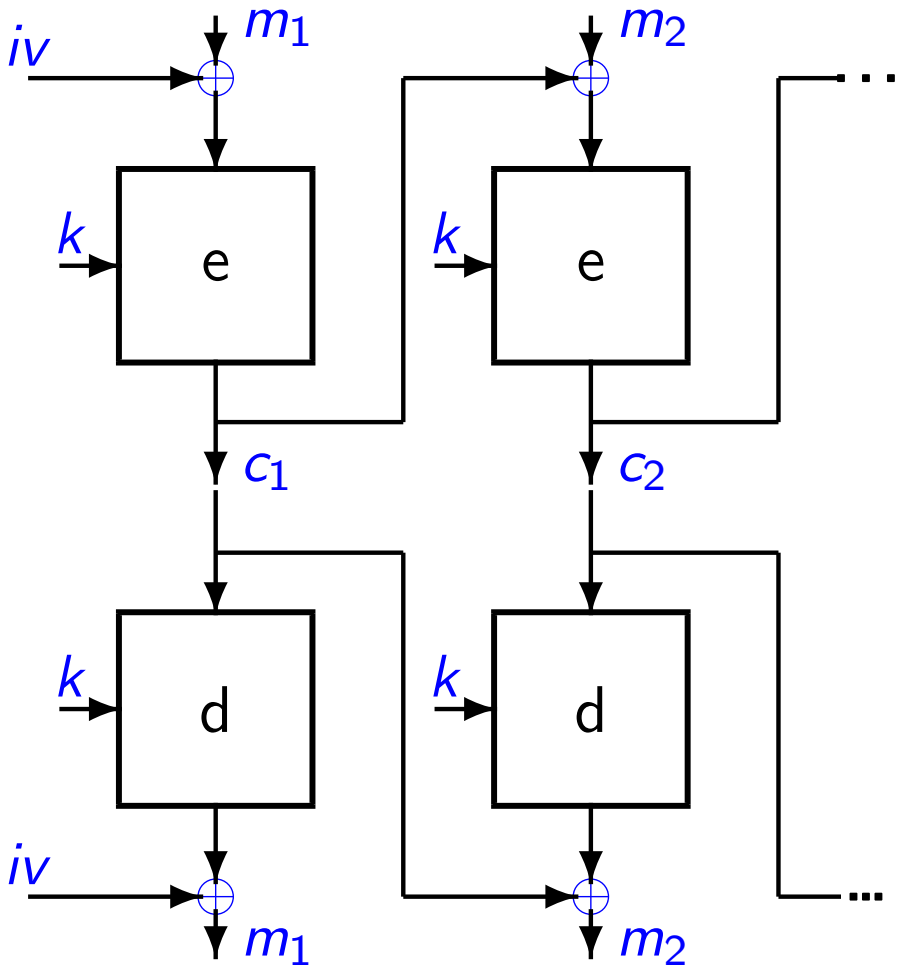
Encryption



How does decryption work?

CBC mode

Encryption and decryption



CTR mode

n and m are sizes in bits