Block cipher modes

block cipher E_k with n bit block size

DES 64 bit
AES 128 bit

$m = m_1 m_2 m_3 \ldots$ each block m_i is n bits (may need to pad)

block cipher modes: how to encrypt each m_i using E_k

ECB (electronic codebook)

$c_j = E_k(m_j)$ $\quad c = c_1 c_2 c_3 \ldots$

simple + natural but **should not be used** (except ...)

EG leaves patterns in c
(same blocks encrypted the same)

EG vulnerable to tampering

CBC (cipherblock chaining)

$c_j = E_k(m_j \oplus c_{j-1})$ $\quad c = c_0 c_1 c_2 c_3 \ldots$ (IV: initialization vector)

decryption: $m_j = D_k(c_j) \oplus c_{j-1}$ $\quad D_k(c_j) = m_j \oplus c_{j-1}$

value of IV should be unpredictable
(same blocks, even across different m, encrypted differently)

EG (silly) 4-bit block cipher $E_k(b_1 b_2 b_3 b_4) = (b_2 b_3 b_4 b_1) \oplus k$

Encrypt $m = 0000\ 1011\ 0000 \ldots$ using $k = 1111$ and

(a) ECB
(b) CBC and $IV = 0011 = c_0$

$m = m_1 m_2 m_3 \ldots$ $\quad m_1 = 0000$ $\quad m_2 = 1011$ $\quad m_3 = 0000$

(a)
$c_1 = E_k(m_1) = E_k(0000) = 0000 \oplus 1111 = 1111$
$c_2 = E_k(m_2) = E_k(1011) = 0111 \oplus 1111 = 1000$
$c_3 = E_k(m_3) = \ldots$ same as for $m_1 \ldots = 1111$

$c = c_1 c_2 c_3 \ldots = 1111\ 1000\ 1111 \ldots$

(b)
$c_1 = E_k(m_1 \oplus c_0) = E_k(0011) = 0110 \oplus 1111 = 1001$
$c_2 = E_k(m_2 \oplus c_1) = E_k(0010) = 0100 \oplus 1111 = 1011$ ($m_2 = 1011$, $c_1 = 1001$)
$c_3 = E_k(m_3 \oplus c_2) = E_k(1011) = 0111 \oplus 1111 = 1000$ ($m_3 = 0000$, $c_2 = 1011$)

$c = c_0 c_1 c_2 c_3 \ldots = 0011\ 1001\ 1011\ 1000 \ldots$