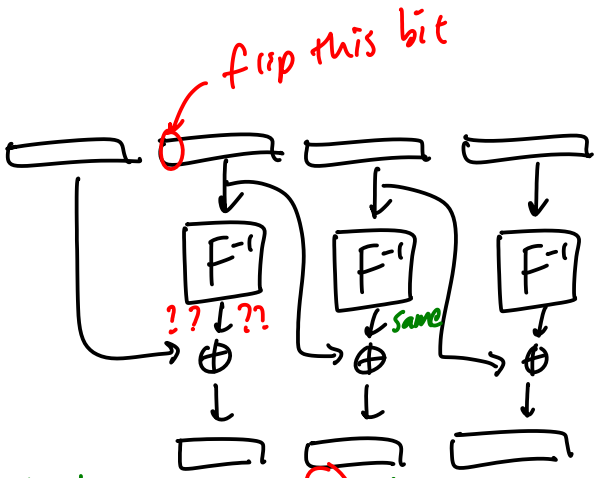
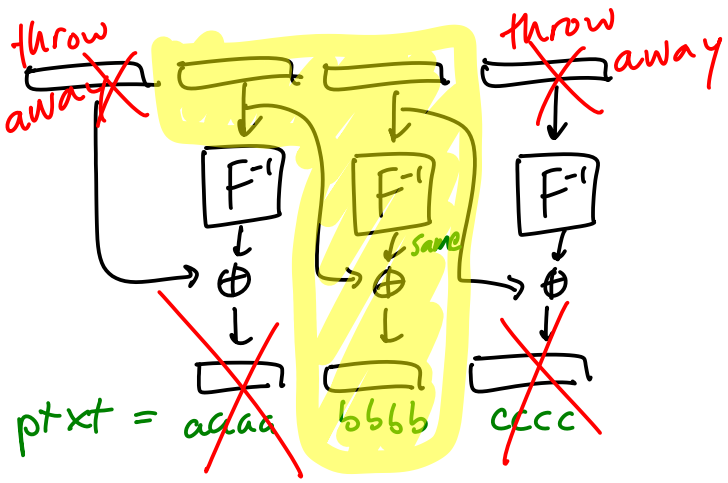
Padding Oracle

Malleability (of CBC)

CBC Decryption





Given $c_0\, c_1 \cdots c_\ell$ which decrypts to $m_1 \cdots m_\ell$

c_{i-1} c_i Decrypt to m_i

$X \oplus c_{i-1}$ c_i Decrypts to $X \oplus m_i$

Padding oracle tells me whether secret ptxt ends in { 01, 00 02, 00 00 03, ⋮ }

padding oracle + malleable CBC mode

⇒ tell me whether secret ⊕ x ends in { 01, 00 02, ⋮ }

for any x of MY choice

Demo: Mike has 4-byte secret [S]

Ask him any x (4-byte value), he will tell you whether S⊕X ends in { 01, 0002, 000003, 00000004 }

X	Mike
00…00	NO
ff…ff	NO
11…11	NO
00 00 00 01	NO
… 02	NO
⋮	⋮
00 00 00 0f	NO
⋮	⋮
00 00 00 c0	YES
⋮	⋮
00 00 00 ff	NO

last byte of s either 01⊕c0, 02⊕c0, 03⊕c0, 04⊕c0

↓ suppose last byte of s = c2

X = 00 00 00 c3 should have said YES too because last byte of S⊕X = 01

X	Mike
00 00 01 c3	NO
00 02 c3	NO
00 03 c3	NO
⋮	
00 00 49 c3	YES

So: S = [c1]

Want { ⊕ X = 00 00 [??] c3

? ? 00 02

S = [49 c1]

⊕ X [00 00 49 c3]

?? ?? 00 02