Chosen Ciphertext Attacks

A particular ctxt leaks nothing about its ptxt
... even when Adv can decrypt ANY OTHER ctxt

Def:

```
$k \leftarrow$ KeyGen
SEEN = $\emptyset$
CHALLENGE($m_L, m_R$):
    $c = $ Enc($k, m_L$)
    add c to SEEN
    return c
GETDEC(c):
    if $c \in$ SEEN ret null
    ret Dec(k,c)
```

$\approx$

```
$k \leftarrow$ KeyGen
SEEN = $\emptyset$
CHALLENGE($m_L, m_R$):
    $c = $ Enc($k, m_R$)
    add c to SEEN
    return c
GETDEC(c):
    if $c \in$ SEEN ret null
    ret Dec(k,c)
```

Idea: Malleability = given c, encryption of unknown m

can produce c′ so that Dec(k, c′) has known relationship to m

Ex: CBC mode: $c_0 c_1 \cdots c_\ell = \text{Enc}(k, m_1 \cdots m_\ell)$

then $\text{Dec}(k, (c_{i-1}, c_i)) = m_i$

$\text{Dec}(k, (x \oplus c_{i-1}, c_i)) = m_i \oplus x$

CCA attacks:

- OTP is not CCA secure

malleable? given $c = k \oplus m$ (m unknown)

then $c \oplus x = k \oplus (m \oplus x)$

$= \text{Enc}(k, m \oplus x)$

Attack:

choose $m_L \neq m_R$, $x \neq 0^\lambda$

$c = \text{CHALLENGE}(m_L, m_R)$

$m^* = \text{GETDEC}(c \oplus x)$

return $m_L \oplus x \overset{?}{=} m^*$

$c = k \oplus m_L$

$\text{Dec}(k, c \oplus x)$

$= m_L \oplus x$

$= m^*$

$c = k \oplus m_R$

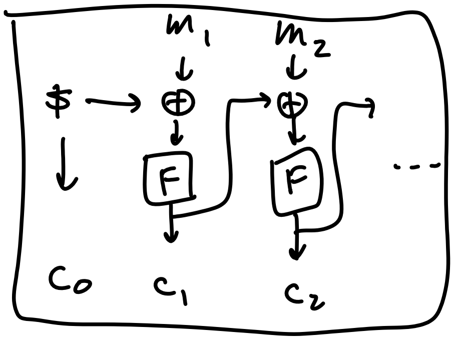
$m^* = \text{Dec}(c \oplus x)$

$= m_R \oplus x$

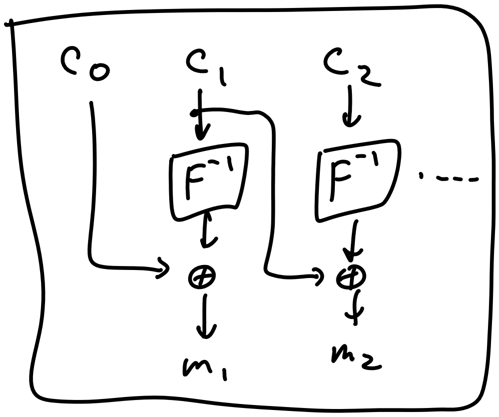
$\neq m^L$

- CBC mode: not CCA secure

Enc



Dec

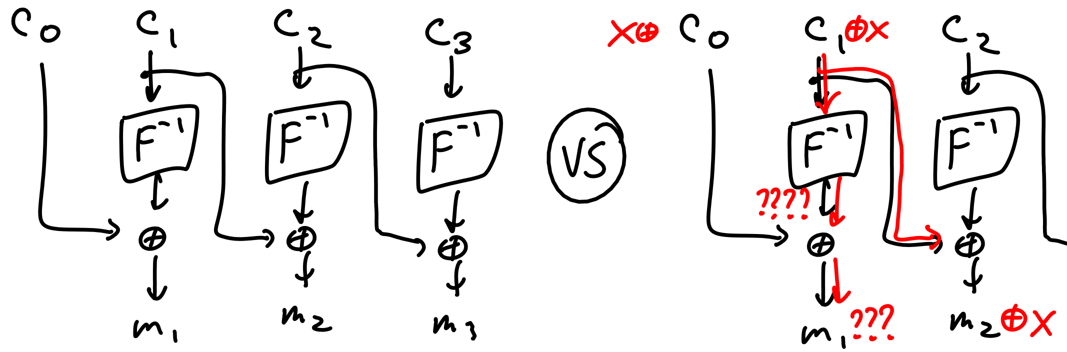


Malleable: given $c_0 c_1 c_2 c_3 = \text{Enc}(m_1 m_2 m_3)$

"flip some bits" in c_1

$\Rightarrow$ $c' = c_0 \| c_1 \oplus x \| c_2 \| c_3$

Q $\longrightarrow$ How is $\text{Dec}(c')$ related to $m_1 m_2 m_3$?



Ⓐ → m_1 clobbered (out of Adv's control)

m_2 becomes $m_2 \oplus X$

m_3 same

Attack:

pick $m_1, m_2, m_3 \neq m_3'$, $X \neq 0^\lambda$

$c_0 c_1 c_2 c_3 = \text{CHALL}\begin{pmatrix} m_1 m_2 m_3, \\ m_1 m_2 m_3' \end{pmatrix}$

$\hat{m}_1 \hat{m}_2 \hat{m}_3 = \text{GETDEC}(c_0 \| c_1 \oplus X \| c_2 \| c_3)$

return $\hat{m}_3 \overset{?}{=} m_3$

"CBC malleable in a way that leaves m_3 unchanged"

Attack:

pick $m_1, m_2 \neq m_2', m_3$, $X \neq 0^\lambda$

$c_0 c_1 c_2 c_3 = \text{CHALL}\begin{pmatrix} m_1 m_2 m_3, \\ m_1 m_2' m_3 \end{pmatrix}$

$\hat{m}_1 \hat{m}_2 \hat{m}_3 = \text{GETDEC}(c_0 \| c_1 \oplus X \| c_2 \| c_3)$

return $\hat{m}_2 \overset{?}{=} m_2 \oplus X$

"malleable in a way that XORs m_2 by known value"

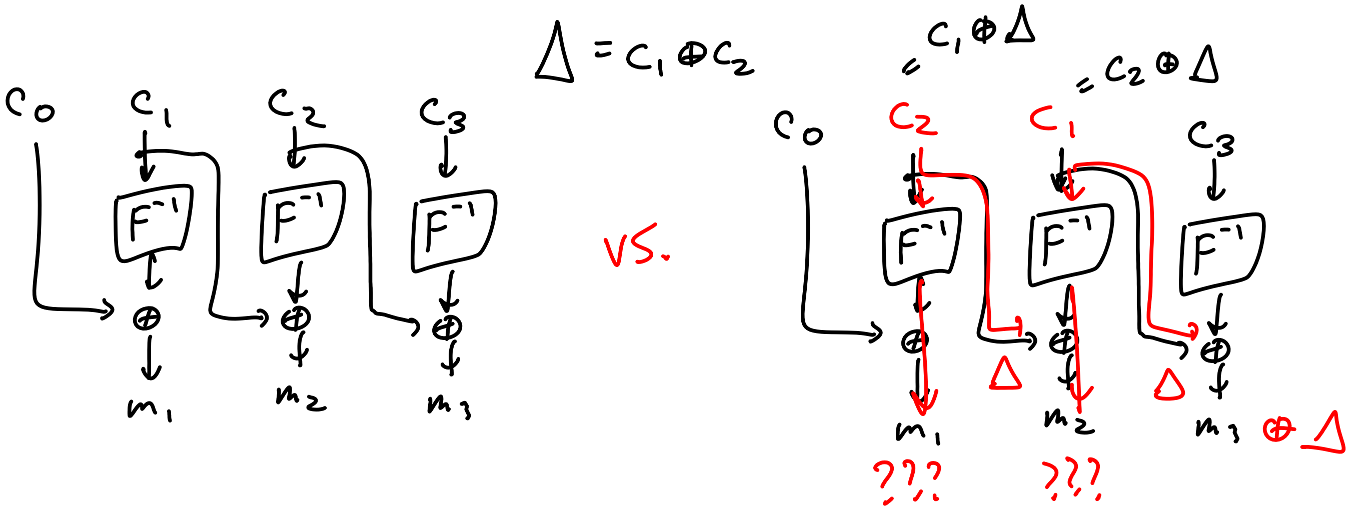
Attack:

pick $m_1 m_2 m_3 \neq m_3'$

$c_0 c_1 c_2 c_3 = \text{CHALL}\begin{pmatrix} m_1 m_2 m_3, \\ m_1 m_2 m_3' \end{pmatrix}$

$\hat{m}_1 \hat{m}_2 \hat{m}_3 = \text{GETDEC}(c_0 \| c_2 \| c_1 \| c_3)$

return $\hat{m}_3 \overset{?}{=} m_3 \oplus \underbrace{c_1 \oplus c_2}_{\text{“}\Delta\text{”}}$


Δ = c₁ ⊕ c₂
c₀
c₁
c₂
c₃
F⁻¹
F⁻¹
F⁻¹
m₁
m₂
m₃
vs.
= c₁ ⊕ Δ
= c₂ ⊕ Δ
c₀
c₂
c₁
c₃
F⁻¹
F⁻¹
F⁻¹
Δ
Δ
m₁
m₂
m₃ ⊕ Δ
???
???