**CPA-Secure Modes & Malleability**

**Last time:** CPA Security (chosen plaintext attack)

"Cannot distinguish Enc(k,m_0) from Enc(k,m_1), even when given ability to obtain encryptions of arbitrary chosen plaintexts."

**Observation:** Encrypting same message twice must result in different values (for CPA security)

\[ \rightarrow \text{Enc procedure must use extra randomness} \]

**"Modes" for block ciphers**

ECB mode \( \Rightarrow \) send each block independently thru block cipher

(not CPA secure)

CBC mode (cipher-block chaining)

---

**Enc:**

Choose random block (IV)

\[ n_1 \quad m_2 \quad m_3 \quad m_4 \quad \ldots \]

Input / plaintext

Block length

\[ \oplus \quad \oplus \quad \oplus \quad \oplus \quad \ldots \]

\[ F_k \quad F_k \quad F_k \quad F_k \quad \ldots \]

\[ c_0 \quad c_1 \quad c_2 \quad c_3 \quad c_4 \quad \ldots \]

Output / ciphertext

---

Initialization vector
Fact: CBC mode (random IV) is CPA-secure (in fact, output blocks all "look random")

Others:

OFB = output feedback

"Use IV, \( F_k(IV) \), \( F_k(F_k(IV)) \), ... as one-time pad on plaintext"

CTR = counter

"Use \( F_k(IV) \), \( F_k(IV+1) \), \( F_k(IV+2) \), ... as one-time pad on plaintext"

Malleability:

Myth: \( m = \text{Dec}(k, c) \) means \( m \) is a message that key-owner agrees with

(how else could anyone come up with \( c \) if not with help from key-owner ?)
Counterexample:

Have OFB-mode encryption of “attack at dawn”
Can I come up with an encryption of “attack at dusk”??

OFB: \[ \text{ciphertext} = \text{plaintext} \oplus \text{mask} \]
\[ \rightarrow \text{solve for mask} \]
\[ \text{ciphertext} = \text{plaintext} \oplus \text{mask} \]