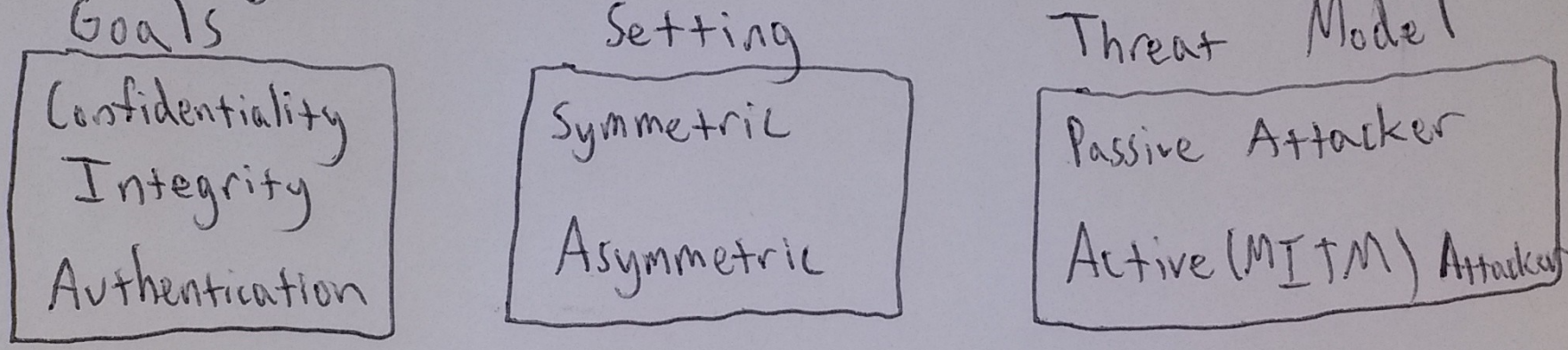
CS 161 Midterm 2 Review

Grant, Frank, Rishabh

- Kerckoff Principle: Attacker knows everything about defense/protocol except for secret inputs
- Three layers to consider w/ crypto:



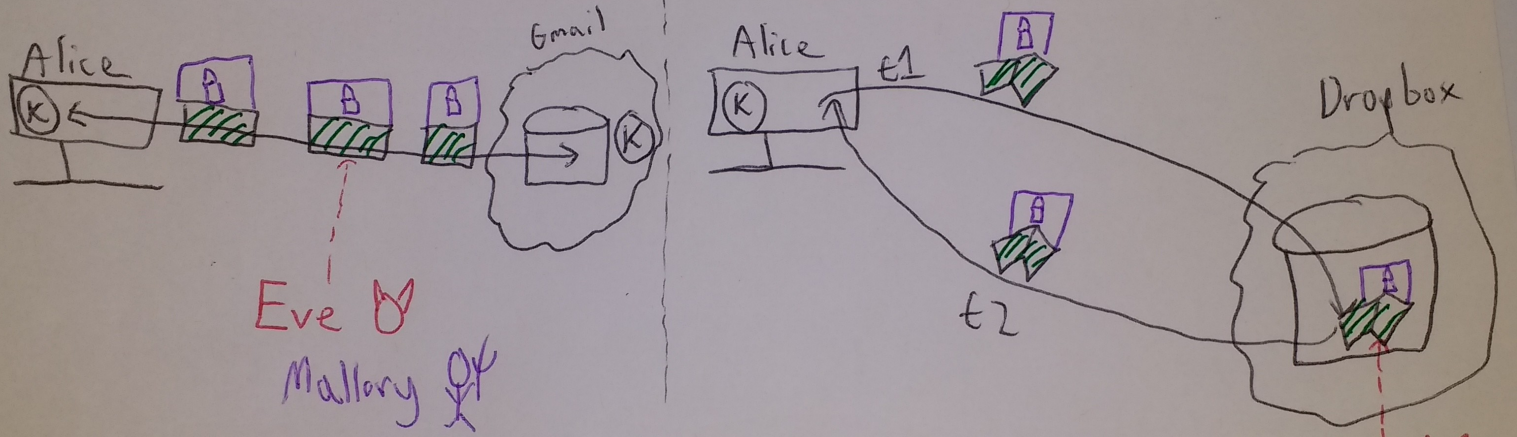
Conf: Do I need to keep data secret/private?

Integrity: Do I need to check if data/msg was modified/tampered?

Authentication: Do I need to check identity of something/ check if data came from particular src?

Symmetric Setting

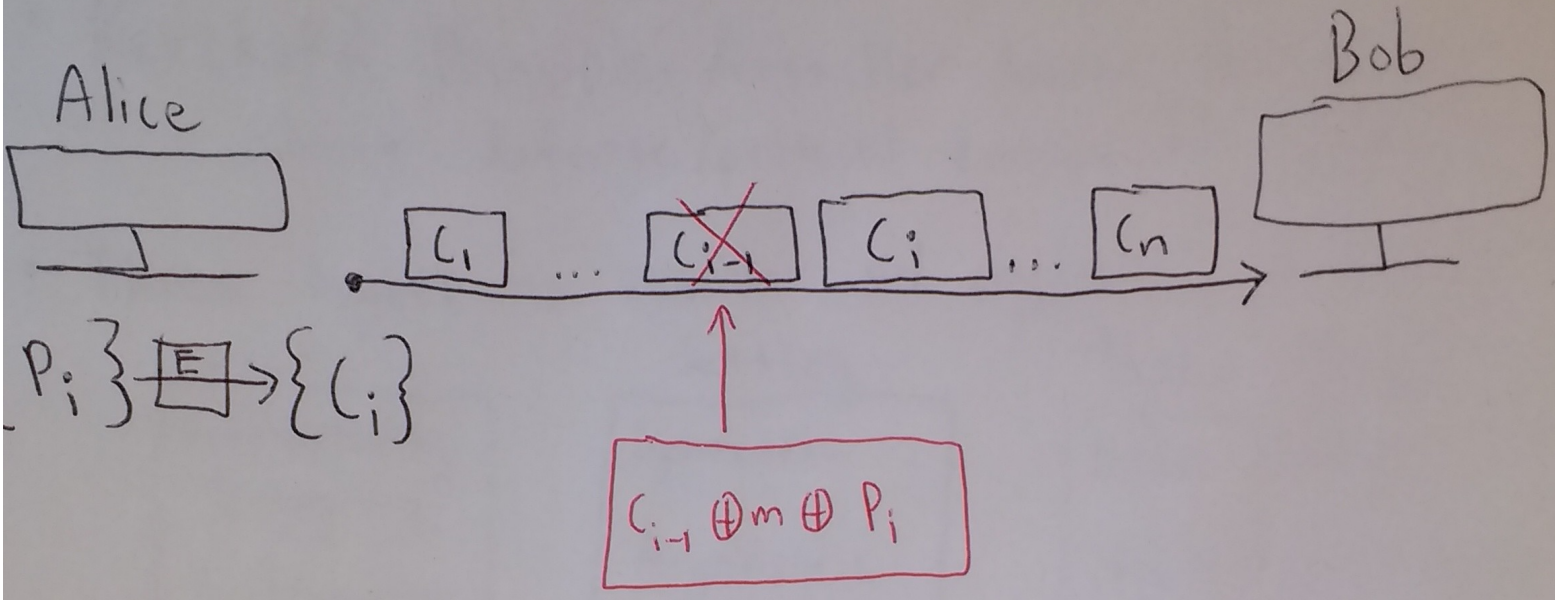
Common Scenario 1 | Common Scenario 2



- Encrypt to provide confidentiality (no integrity!)
  - Block ciphers
  - Stream ciphers
- MACs provide integrity (no confidentiality!)

Spring 2015 MT 2

Question #2



a) • Attack Fails.

Decrypt in ECB: $P_i = AES^{-1}(K, C_i)$

Bob's $P_{i-1} = AES^{-1}(K, C_{i-1} \oplus m \oplus P_i) \neq m$

~~Zero~~ basically garbage/rand str

• Only C_{i-1} decrypts incorrectly

Spring 2015 MT 2

Question #2

a) [redacted]

CBC encryption:

$C_i = AES(K, P_i \oplus C_{i-1})$ where $C_0 = IV$

b) CBC decryption:

$$P_i = AES^{-1}(K, C_i) \oplus C_{i-1}$$

- Attack succeeds:

Bob decrypts $P_i = AES^{-1}(K, C_i) \oplus C'_{i-1}$

$$P_i = AES^{-1}(K, AES(K, P_i \oplus C_{i-1})) \oplus C'_{i-1}$$

$$= P_i \oplus C_{i-1} \oplus (C_{i-1} \oplus m \oplus P_i)$$

$$= m \oplus (P_i \oplus P_i) \oplus (C_{i-1} \oplus C_{i-1})$$

- C_i decrypts incorrectly (to m)

  C_{i-1} decrypts incorrectly (decrypting Mallory's C'_{i-1})

2015 MT2 Q2

c) Note question for this part is different than a & b!

Mallory replaces C_i w/ C_i' where

$$C_i' = C_i \oplus P_i \oplus m$$

Now Bob will decrypt C_i' instead of C_i to get

$$P_i = AES(K, x) \oplus C_i'$$

$$= AES(K, x) \oplus (C_i \oplus P_i \oplus m)$$

$$= m \oplus C_i \oplus (P_i \oplus AES(K, x))$$

$$= m \oplus C_i \oplus C_i$$

$$= m$$

, where $AES(K, x)$ corresponds to the full "pseudorandom part" generated by encrypting the IV & ctr's for the message

$P_i \oplus AES(K, x)$ — CTR-mode encryption

- Only C_i decryption fails