# Chapter 3
# Symmetric Key Crypto & Data Integrity
# Sep 6th

Part 1 ≥E Cryptography

# Data Integrity

- **Integrity** —prevent (or at least detect) unauthorized modification of data
- Example: Inter-bank fund transfers
  - Confidentiality is nice, but integrity is critical
- Encryption provides **confidentiality** (prevents unauthorized disclosure)
- Encryption alone does **not** assure integrity (recall one-time pad and attack on ECB)

# MAC

- Message Authentication Code (MAC)
  - Used for data **integrity**
  - Integrity **not** the same as confidentiality
- MAC is computed as **CBC residue**
  - Compute CBC encryption, but only save the final ciphertext block

# MAC Computation

- MAC computation (assuming N blocks)

$$C_0 = E(IV \oplus P_0, K),$$

$$C_1 = E(C_0 \oplus P_1, K),$$

$$C_2 = E(C_1 \oplus P_2, K), \ldots$$

$$C_{N-1} = E(C_{N-2} \oplus P_{N-1}, K) = MAC$$

- MAC sent along with plaintext
- Receiver does same computation and verifies that result agrees with MAC
- Receiver must also know the key K

# Why does a MAC work?

- Suppose Alice has 4 plaintext blocks
- Alice computes

$$C_0 = E(IV \oplus P_0, K),\ C_1 = E(C_0 \oplus P_1, K),$$

$$C_2 = E(C_1 \oplus P_2, K),\ C_3 = E(C_2 \oplus P_3, K) = MAC$$

- Alice sends $IV, P_0, P_1, P_2, P_3$ and $MAC$ to Bob
- Suppose Trudy changes $P_1$ to $X$
- Bob computes

$$C_0 = E(IV \oplus P_0, K),\ \mathbf{C_1} = E(C_0 \oplus X, K),$$

$$\mathbf{C_2} = E(\mathbf{C_1} \oplus P_2, K),\ \mathbf{C_3} = E(\mathbf{C_2} \oplus P_3, K) = \mathbf{MAC} \neq MAC$$

- Error **propagates** into **MAC** (unlike CBC decryption)
- Trudy can't change **MAC** to $MAC$ without key $K$

# Confidentiality and Integrity

- Encrypt with one key, compute MAC with another
- Why not use the same key?
  - Send last encrypted block (MAC) twice?
  - Can't add any security!
- Using different keys to encrypt and compute MAC works, even if keys are related
  - But still twice as much work as encryption alone
- Confidentiality and integrity with one "encryption" is a research topic

# Uses for Symmetric Crypto

- Confidentiality
  - Transmitting data over insecure channel
  - Secure storage on insecure media
- Integrity (MAC)
- Authentication protocols (later…)
- Anything you can do with a hash function (upcoming chapter…)

# Next …
# Public Key Cryptography