Practice Exercises

The following exercises will begin to help you understand why there are multiple types of encryption and block cipher modes. For the scenario exercises, there can certainly be more than one answer to the question, depending on how the scenario functions or is used, or what would be considered “acceptable loss” should there be corrupted ciphertext.

Reading Material & Utilities

- Block Cipher Modes of Operation
- Galois/Counter Mode (GCM) of Operation
- Stream Ciphers
- An Overview of Symmetric Encryption and the Key Lifecycle
- CyberChef - All in One Tool for analyzing data formats, baking formulas, encryption mechanisms, etc.

Exercises

1. For the following scenarios, which type of symmetric encryption do you think would be better (block cipher or stream cipher) for encrypting the data?
    a. Video chats
    b. Text messaging
    c. Netflix/Hulu
    d. Downloaded video (no streaming)
    e. Thesis paper
    f. Phone calls
    g. Log files
    h. Pictures
    i. Steam/PC Game Files
2. How much data could be lost if a byte of ciphertext is changed,
    a. For CBC?
    b. For CTR?
    c. For GCM?
3. How much data could be lost if a byte of ciphertext is removed (modified ciphertext is one byte smaller in length),
    a. For CBC?
    b. For CTR?
    c. For GCM?
4. For the following scenarios, which of the following modes of operation do you think work best for securing the data? Modes of Operation: ECB, CBC, CTR, GCM
    a. Text Messages
    b. Audit Logs
    c. Videos/Pictures
    d. Hashed Passwords