Homework 6: Due Monday, March 4th

Peter Schaefer

4. **Galois/Counter Mode (GCM)**
    b. **Describe how the mode of operation works in complete sentences.**

GCM works by combining the counter mode of operation with Galois field multiplication for authentication.

The first step is initialization; GCM requires an initialization vector (IV) and a secret key. It is important that this IV is unique for each batch of encryption. The plaintext is divided into blocks, typically 128 bits for AES. A counter is then used to generate the encryption text for each block. The initial counter value is derived from the IV, and each subsequent value is an incrementation of this initial counter value. Each plaintext block is encrypted using the block cipher algorithm in counter mode. Simultaneously, GCM computes a MAC by using the ciphertext and possible associated data. This tag is generated using Galois field multiplication. At the end of the encryption, the authentication tag is appended to the ciphertext.

Decryption is conducted using the same IV and key. The ciphertext is divided into blocks (typically 128 bit), and each block is decrypted using the block cipher in counter mode. As this is done, the receiver computes the authentication tag from the ciphertext data. At the end of decryption, if the computed tag matches the received tag, the ciphertext is considered authenticated, and the plaintext is recovered. Otherwise, the ciphertext is considered tampered and invalid.

    c. **What are the known strengths and/or weaknesses of the mode of operation?**

<u>Advantages</u>

i. GCM offers both encryption and authentication in one system.
ii. GCM is both computationally and bandwidth efficient, which makes it suitable for use in a wide range of applications.

<u>Disadvantages</u>

iii. GCM requires proper IV management to prevent IV reuse, which can compromise security.