Alan Palayil

A20447935

Due Date: February 3rd, 2023

ECE 543

1. What is the playback attack? What is the common practice in protocol design to defend against playback attack?
   - A playback attack is a type of network security attack in which a recorded message or data is replayed to the recipient, masquerading as a legitimate request. This can occur when an attacker intercepts a message, records it, and then re-transmits it later to deceive the recipient into thinking that it is a genuine request.
     To defend against it, protocol designs often include a mechanism for ensuring message freshness, such as timestamps, sequence numbers, or nonces. These unique values help verify that the message is recent and not a replay. This defense is used in various network security protocols like SSL/TLS, IPsec, and Kerberos, to ensure message authenticity and integrity.

2. Why is the public key technology so important for large-scale network security applications?
   - The public key technology is crucial for large-scale network security applications because it provides a secure means of exchanging information over an insecure network. It uses a pair of keys, a public key, and a private key, for encryption and decryption of data. The public key can be freely distributed to others for encrypting messages, while the private key must be kept secret and is used for decrypting messages. This ensures that only the owner of the private key can read the encrypted messages, providing confidentiality, authenticity, and non-repudiation. As a result, public key technology is widely used in various secure network applications, such as digital signatures, SSL/TLS, email encryption, and VPNs.

3. How can you use the same Feistel module (considered as an IC chip) for both encryption and decryption?
   - The same Feistel module in a Feistel cipher can be used for both encryption and decryption by utilizing key inversion. This involves using the original key for encryption and the inverse key for decryption. The inverse key is obtained by swapping the values of the left and right halves of the block and applying the inverse function to each half. The decryption process then performs the reverse operations of the encryption process, undoing the encryption and providing the original data.
     By using key inversion, the same Feistel module can be utilized for both encryption and decryption, making the cipher efficient and versatile.