ECE 543 Quiz 2

Alan Palayil
A20447935
Due Date: 3/24/2023

1. Generating a pair of RSA keys involves the following steps:
   - Choose two distinct prime numbers, p and q.
   - Compute the modulus n as the product of p and q: $n = p * q$.
   - Compute Euler's totient function, $\varphi(n)$, for the modulus n: $\varphi(n) = (p-1) * (q-1)$.
   - Choose a public exponent, e, such that $1 < e < \varphi(n)$ and $\gcd(e, \varphi(n)) = 1$ (i.e., e and $\varphi(n)$ are coprime).
   - Calculate the private exponent, d, as the modular multiplicative inverse of e modulo $\varphi(n)$: $d \equiv e^{-1} \pmod{\varphi(n)}$.
   - The public key is the pair (n, e), and the private key is the pair (n, d).

   The public key is used for encryption, while the private key is used for decryption in the RSA cryptosystem.

2. A man-in-the-middle attack on the Diffie-Hellman protocol occurs when an attacker intercepts and manipulates key exchange messages between two parties, effectively positioning themselves between the communicating parties. The attacker establishes independent key exchanges with each party, deceiving them into believing they are communicating securely with each other, while the attacker can eavesdrop and potentially alter the exchanged data. In the lecture example, Trudy has both g^{AT} and g^{BT} and receives messages from Alice ($T_A=g^A \bmod p$) and sends it to Bob ($T_T=g^T \bmod p$). Bob sends the acknowledgement ($T_B=g^B \bmod p$) and Trudy listens and sends it to Alice ($T_T=g^T \bmod p$).

3. If Alice and Bob already have a shared secret key, the Diffie-Hellman (D-H) technique can provide the following additional benefits:

   - Perfect Forward Secrecy" (PFS): By generating ephemeral keys for each session, the D-H technique can ensure that even if a long-term secret key is compromised, past session keys will not be revealed. This protects the confidentiality of previous communications.
   - Precludes my ability to decrypt a conversation even after successfully compromising both parties once the communication has concluded, or in cases where the private key is held in escrow.
   - For example, in a non-PFS system: Alice selects a key S, encrypts it using Bob's public key, and transmits it to Bob (as in SSL).