Hw5

Jackson Mowry

Tue Sep 30 11:10:39 2025

Diffie-Hellman

1. Describe the Diffie-Hellman Protocol.

   - The Diffie-Hellman is a process of establishing a secure communication channel across an insecure medium. This requires some parameters to be agreed upon beforehand, then each party can pick their own secret. The combination of these agreed upon initial parameters, and their chosen secrets allows for both parties to end up with the same shared secret. The concept can be more simply described as what one key does (encrypt) the other key undoes (decrypt).

2. Show how Mallory can conduct a man-in-the-middle attack when Alice and Bob perform the HD protocol from Question 1.

   - If we assume Mallory can listen to the communications between Alice and Bob, then we can also assume she was able to listen to their initial key sharing process. There is no proof to Alice that Bob is actually Bob, and same for Bob to Alice. Therefore, Mallory can perform the key agreement process with Alice, pretending to be Bob, and with Bob pretending to be Alice. Going forward all communication between Alice and Bob would be tunneled through Mallory, where she could read all messages.

3. What is the recommended key size for the prime modulus p in DH?

   - A number of at least 2048 bits.

4. Why is the recommended size of p for DH so much larger than the recommended key size for AES?

- In order for the math in DH to work the keys have to be mathmatically related, specifically defined by the initial chosen shared values which limit our space. The mathmatical relationship that initially allows us to choose the 2 keys could also be used find the 2 keys if we're able to factor a large number into 2 primes.

RSA

1. Generate RSA key parameters where p=7, q=13, and 2<e<7. Try values for e in order until finding one that will work. Generate d using the extended Euclidean algorithm. Show detailed work. do All your work by hand.

    - p = 7
    - q = 13
    - n = 91
    - tot(n) = 12 = lcm(p-1,q-1)
        - Calculate lcm here
        - (6 * 12) / 6
        - 72 / 6
        - 12
        - The lcm is 12
    - e = 3, gcd(3, 12) = 4
        - Calcuate gcd by hand
        - 12 = 3 * x + 0
        - 12 = 3 * 4 + 0
        - Done, gcd = 4
    - e = 4, gcd(4, 12) = 3
        - Calculate gcd by hand
        - 12 = 4 * x + 0
        - 12 = 4 * 3 + 0
        - Done, gcd = 3
    - e = 5, gcd(5, 12) = 1
        - Calculate gcd by hand, then do extended euclidians
        - 12 = 5 * 2 + 2

  - 5 = 2 * 2 + 1
  - 2 = 1 * 2 + 0
  - done, gcd = 1
  - Working our way back up
  - 5 - 2 * 2 = 1
  - 5 - (12 - 5 * 2) * 2= 1
  - 5 - 12 * 2 - 5 * 4
  - 5 * 5 - 2 * 12
  - 5 and -2, 5 is our MI
- d = 5

2. Identify the RSA public key and the RSA private key.
   - Public key = {5, 91} ({e, n})
   - Private key = {5, 91} ({d, n})