Diffie-Hellman Key Exchange and El Gamal Encryption

Marcio Woitek

Problem 1

▷ The prime modulus (p)
▷ Bob's public key (Y_B)
▷ The primitive root of the prime modulus (a)
▷ The shared key by the protocol (K)

Problem 2

▷ The shared key by the protocol (K)
▷ Bob's private key (X_B) [The instructor used the wrong notation]

Problem 3

Answer: 6

The formula for Alice's public key is

$$Y_A = a^{X_A} \bmod p. \tag{1}$$

Substituting $a = 2$, $p = 11$ and $Y_A = 9$ into this equation, we get

$$9 = 2^{X_A} \bmod 11 \Rightarrow X_A = \mathrm{dlog}_{2,11}\, 9 = 6. \tag{2}$$

Problem 4

Answer: 3

To compute the secret key K, we can use the following equation:

$$K = Y_B^{X_A} \bmod p. \tag{3}$$

By using the values of Y_B, X_A and p, we obtain

$$K = 3^6 \bmod 11 = 729 \bmod 11 = 3. \tag{4}$$

Problem 5

▷ Diffie-Hellman Key Exchange protocol is vulnerable to MITM attack because of the lack of authentication.

Problem 6

▷ El Gamal Encryption includes the message and the key that is used to protect the message, and the key itself is protected against eavesdropping.
▷ El Gamal Encryption uses a prime modulus and a primitive root of the modulus.