CS 463/563: Cryptography for Cybersecurity
Spring 2024
Homework #7
Points: 20

Question 1: [10 points] For the given three cases where **Alice** and **Bob** are trying to establish a shared secret key using **Diffie-Hellman** key exchange protocol, fill the values in the table. Show your work.

Parameter	Case 1	Case 2	Case 3
p, a large prime	11	37	59
α, an integer in {2,3,…, p-2}	6	11	15
p and α are published			
Alice chooses a in {2,3,…, p-2}	4	13	17
Bob chooses b in {2,3,…, p-2}	5	9	20
Alice computes $A = \alpha^a \bmod p$, its public key			
Bob computes $B = \alpha^b \bmod p$, its public key			
Alice and Bob exchange their public keys, A and B			
Alice computes the shared key, $K_{AB} = B^a \bmod p$			
Bob computes the shared key, $K_{AB} = A^b \bmod p$			
Verify that both the shared keys are identical			

Question 2: [10 points] For the given three cases where **Alice** is trying to send encrypted data to **Bob**, and **Bob** is trying to decrypt it, using **Elgamal encryption scheme**, fill the values in the table. Show your work.

Parameter	Case 1	Case 2	Case 3
Bob chooses p, a large prime	11	31	59
Bob chooses α, **primitive element** in Z^*_p	7	3	2
Bob chooses $K_{pr} = d \in \{2,3, ..., p-2\}$	6	9	3
Bob computes $K_{pub} = \beta = \alpha^d \bmod p$			
p, α, and β are sent to Alice			
Alice chooses i in {2,3,…, p-2}	4	5	7
Alice computes $K_E = \alpha^i \bmod p$			
Alice computes $K_M = \beta^i \bmod p$			
Alice's message to send is $x \in Z^*_p$	7	7	9
Alice encrypts message x, $y = x*K_M \bmod p$			
Alice sends K_E and y to Bob			
Bob computes $K_M = K_E^d \bmod p$			
Verify that Bob indeed computed the same K_M as what Alice did above			
Bob computes $K_M^{-1} \bmod p$			
Bob computes $x = y* K_M^{-1} \bmod p$			
Verify that Bob indeed decrypted x correctly			

Note: $\mathbf{Z^*_n}$ is a set of elements with multiplication operation, and integers less than that are relatively prime to **n**. For example, if **p =19**, $\mathbf{Z^*_{19} = \{1,2,3,4,\ldots,16,17,18\}}$. Here, since p is a prime, $\mathbf{Z^*_p}$ will also be **{1,2,3,…,p-1}**