CSE015-HW05

Shulang Ning

November 20, 2017

1 Question 1

I need to send you the value of B which $B = g^b \bmod p$. g and p are the public key, and b is my private key which cannot show you, and it is same as a which is your private key. Those two value a and b are used to decrpyt the cipher with the exchange key s, which $s = B^a \bmod p = A^b \bmod p$. However, in the question, there is lack of a public key s. In this case, I cannot make sure that my private key b is useful or not to calculate s, and we have to get the same s. The B that I can show you is only worked when we got the same s. I just assume that we have a s which is 1051, and my B is 3152

2 Question 2

They just got the public key which are A, B, g, p, and s, and need to solve the private key which are a and b. There are two ways to solve them. The first one is using s to solve a and b. Because they know the value of s, A, B, and p , and they can use $s = B^a \bmod p = A^b \bmod p$ to solve a and b by letting the s same in two formula. The second way to solve a and b is to use the formula $A = g^a \bmod p$ and $B = g^b \bmod p$, and use the way called formula backstepping to solve a and b. If they got the public key before Alice and Bob tell to each other, Eve can change the public key and even change the information that Alice and Bob want to send to each other. First, Eve can choose the private key c and d by himself, and calculate the C and D, and send C to Alice and D to Bob. Also, Eve have two s, one is same with Alice, and one is same with Bob. In this case, Eve can understand both of Alice's and Bob's information.

3 Question 3

Using $A = g^a \bmod p$ to solve a.