Patrick Austin

4/29/2018

CS 491 1001 Homework 4

1.

a. The public key for user A is calculated via A = ga mod p, where g is the primitive root, which equals 7, a is the private key of user A, 5, and p is the common prime, 71. So   
A = 75 mod 71 = 51, which is user A’s public key.

b. Likewise, B = gb mod p = 712 mod 71 = 4, which is user B’s public key.

c. The shared secret key is calculated for user A via Ab mod p = 5112 mod 71 = 30. User B calculates the secret key via Ba mod p = 45 mod 71 = 30. These values match, as they should, and the value 30 constitutes the shared secret key.

2.

a. First, K must be calculated via K = (YB)k mod q = 32 mod 71 = 9. Then C1 must be calculated via C1 = αkmod q = 72 mod 71 = 49. Then C2 must be calculated via   
C2 = KM mod q = (9 \* 30) mod 71 = 57.

The ciphertext is the pair of values (C1,C2) i.e. (49, 57).

b. C1 = 59 = αk mod q = 7k mod 71. So we must solve 59 = 7k mod 71 for k in order to get the value necessary to generate C2. To solve this discrete logarithm we simply enumerate all possible solutions. In this case we can stop at 73 mod 71 = 343 mod 71 = 59, so k = 3.

With the value of k, we can then generate K. K = 33 mod 71 = 27.

With the value of K, we can then generate C2. C2 = KM mod q = 27 \* 30 mod 71 =   
810 mod 71 = 29. So the value of C2 is now 29.

3.

a. User B’s public key PB = NB \* G = 7 \* (2,7) = (7,2).

b. The ciphertext Cm = { kG, Pm + kPB} = { 3\*(2,7), (10,9) + 3\*(7,2) } = { (8,3) , (10,2) }.

c. Pm is recovered by solving Pm = (Pm + kPB) - (NB\*(kG)) = (10,2) - (7\*(8,3)) = (10,9), so we retrieve the original message, as expected.