# Network Security

# Homework 6

## CHANG LIU

## chang.liu@jhu.edu

# April. 22, 2012

**1. Use Fermat’s Theorem to find**

**(a) 3201 mod 11**

In the Fermat’s Theorem we know that if p is prime and a is a positive integer not divisible by p, we will have:



Thus we have:



Times both side with 3, we have:



**(b) a number x between 0 and 28 with** 

**2. (a) Determine Φ(n) for (a) n= 41, (b) 27, (c) 231 and (d) 440**

**n = 41**

**3. Users A and B use the Diffie-Hellman key exchange technique with a common prime q=71 and a primitive root α=7.**

**(a) If user A has private key XA=5, what is A’s public key YA?**

A’s public key can be calculated as following:



**(b) If user B has the private key XB=12, what is B’s public key YB?**

B’s public key can be calculated as following:



**(c) What is the shared secret key?**



Thus the shared secret key is 30.

**4. Consider a Diffie-Hellman scheme with a common prime q=11 and a primitive root α=2.**

**(a) Show that 2 is the primitive root of 11**



Thus we know that 2i mod 11 for 0<i<11 contains all the numbers from 1 to 10, the size of this set =, the order of q.

Hence 2 is a primitive root of 11.

**(b) If user A has public key YA=9, what is A’s private key XA?**

From (a) we know that , thus the XA = 6.

**(c) If user B has a public key YB=3, what is the secret key K shared with A?**



Thus the secret key is 3.

**5. Consider ElGamal scheme with a common prime q=71 and a primitive root α=7.**

**(a) If user B has a public key YB = 3, and A chose the random integer k = 2, what is the ciphertext of M = 30?**



Thus the ciphertext is (49, 57).

**(b) If A now chooses a different value of k so that the encoding of M =30 is C = (59, C2), what is the integer C2?**

We know that



Thus the k = 3, then we have:



Thus C2 = 29