Cryptography Homework 6

Diffie-Hellman Key Exchange

# Required Reading

Cryptology6 slides  
This is a good, non-mathematical description of Diffie-Hellman. <https://www.youtube.com/watch?v=NmM9HA2MQGI>  
Here is the same person describing the math. <https://www.youtube.com/watch?v=Yjrfm_oRO0w>

<https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange>

Do this lab in groups of two (or three if there is an odd number of students.) You can also do this by yourself, you just have to be both Alice and Bob…

This lab leads you through the process of a Diffie-Hellman Key Exchange (DHKE). If you get confused, look at the form you are filling out on page 2. It can give you an overview.

# Select p and α

Working together select a prime number, p, where q = (p-1)/2 is also prime. You can use a list of the first 1000 prime numbers from <https://primes.utm.edu/lists/small/1000.txt>. You should be able to pick a prime greater than 200 that meets the criteria within a few attempts. (Or, you can write a short Python script, see the end of this document.)

Because you have chosen a “safe” prime number, α can be almost anything you wish. It cannot be 1, or p-1, because they form their own subgroup with 1 and p-1 as the only members. The other subgroup, which you will use, contains all numbers in {2 … q-1}. (Remember, q = (p-1)/2.) Usually α is set to a small number, but any number in the group should work.

Record your choices for p and α.

# Select your private keys

Each person should select their own private exponent (if there are three in the group, two select one exponent while one selects another exponent.) The exponent (a or b, depending on who is Alice and who is Bob) should be in the range 2 < a < q-1.

# Compute and share your public keys

Each person should compute their public key, A = αa mod p, or B = αb mod p. Share your key with the other person in the group. Note: the entire key consists of (p, α, and A) or (p, α, and B)

# Compute the session key

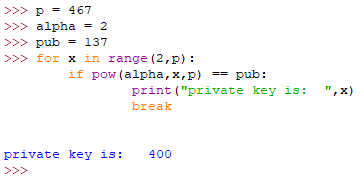
Alice should take Bob’s public key, B, to the power of her private key, a.  
session key = Ba mod p = αab mod p

Bob should take Alice’s public key, A, to the power of her private key, b.  
session key = Ab mod p = αab mod p

Compare your keys. They should be the same.

# Crack the private keys

Since your prime number, p, is small, you should be able to solve the discrete logarithm problem by brute force. Here is some Python code that tries every value of x until it solves pub = alphax mod p. It is taken from the example for Alice’s key in the slides. Demonstrate that if Eve solves this problem she can derive the session key.



# Hand In

1) Fill the blanks in the form below for the DHKE you did with your neighbor. Also, hand in a screenshot of your Python script breaking the key. Remember, to compute  
αa mod  
use  
pow(α, a, p).

p \_\_\_\_\_\_\_\_\_\_\_

α \_\_\_\_\_\_\_\_\_\_\_

**Alice**

Select a \_\_\_\_\_\_\_\_\_\_\_ (Private)

Compute A \_\_\_\_\_\_\_\_\_\_\_ A = αa mod p (Public)

Give A to Bob

**Bob**

Select b \_\_\_\_\_\_\_\_\_\_\_ (Private)

Compute B \_\_\_\_\_\_\_\_\_\_\_ B = αb mod p (Public)

Give B to Alice

**Alice computes key** = Ba mod p (she picked a, Bob gave her B ) \_\_\_\_\_\_\_\_\_\_\_

**Bob computes key** = Ab mod p (he picked b, Alice gave him A) \_\_\_\_\_\_\_\_\_\_\_

Now that Alice and Bob have the same key, they could transfer data with a symmetric algorithm like AES.

2) Attach a screenshot of you breaking the private key. (Hint: use a Python for loop that tests all values of αa mod p until you find the one that equals A. Finding b that gives you B in αb mod p works too. There’s an example of this in Crypto2 slide 11 brute force, except use pow(alpha, i, p) == A instead of a \* i % n == 1 )

3) If p = 19, what is a good choice for α? (Hint: Adjust the code in slide 11, “Python Example, p = 17, α = 3, 2, and 16” for p = 19. Try different values for alpha until you find one that creates a large subgroup.)

# Appendix: Python script to pick a prime, p, where (p-1)/2 is also prime.

#Uses the isPrime function from PyCryptodome

from Crypto.Util.number import isPrime

# check numbers starting at 99 to see if they are prime

# only odd numbers can be prime, so use range(99, 6999, 2)

# stopping at 7000 will get about 900 primes

primes = [x for x in range(99, 6999, 2) if isPrime(x)]

#check to see if (p-1)/2 is a prime so p is "safe"

safe = []

for p in primes:

if isPrime( int((p-1)/2) ):

safe.append(p)

print('Some safe primes are:')

print(safe)

