Homework Assignment 5
Diffie-Hellman Key Exchange

Pedro Damian Sanchez Jr

Sunday, November 19 2017

Private Key

Assume $A = g^a \bmod p$.

Public Keys

Assume $p = 9433$, and, $g = 5$.

Exchange

Transmission $A = 1218$ is recieved.

Question 1

What do you need to send me, in order for us to complete the exchange of the key? Show all your work.

Question 1 Solution

Assume $B = g^b \bmod p$; if I choose $b = 6$ then:

$$\begin{aligned} B &= (5)^{(6)} \bmod 9433 \\ &= 15625 \bmod 9433 \\ &= 6192 \end{aligned}$$

Once I transmit $B = 6192$ we must both arrive at the same "s" by computing the that $[s = A^b \bmod p]$ for me, and, $[s = B^a \bmod p]$ for you.

Question 2

If Trudy, the intruder and Eve, the eavesdropper have intercepted all the our communications above, how would they go about recovering the key that we exchanged? Be very specific.

Question 2 Solution

Since the private keys "a" and "b" aren't known to either Trudy or Eve, they would first have to compute the value of either of those two keys to decrypt all future transmissions.

Question 3

(Bonus question) What is the value of my private key a? How much work was required to find it?

Question 3 Solution

$$\text{Private Key } a = 681$$

To find that value, an algorithm must be implemented to test all numbers between 1 and 9433.