CSE15 Discrete Mathematics
Homework 5

Angelo Kyrilov

Fall, 2017

Diffie–Hellman Key Exchange

Suppose we wish to communicate securely over a public channel. In order for that to happen, we need to have a way of exchanging encryption keys over the insecure medium available. We have agreed to use Diffie–Hellman to accomplish this.

Public Key

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

Private Keys

Assume that I have chosen my private key a, and that I have computed $A = g^a \bmod p$.

Exchange

Assume that I have transmitted $A = 1218$.

Exercises

1. What do you need to send me, in order for us to complete the exchange of the key? Show all your work.
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.
3. (Bonus question) What is the value of my private key a? How much work was required to find it?