Diffie-Hellman Key Exchange

Prepared by: Roy Geoghegan
Undergraduate Research Assistant
Department of Computer Science
Jackson State University, Jackson, MS

Faculty Mentor: Dr. Natarajan Meghanathan

Diffie-Hellman Key Exchange

The Diffie-Hellman Key Exchange algorithm is a simple algorithm for agreeing on a key to use over an insecure connection.

Diffie-Hellman Key Exchange

The key that we will be using today will be the key to a Caesar Cipher (similar to ROT-13). The agreed upon key will be the number of places to shift to encrypt/decrypt a message.

Setup

To get ready for this module, divide into teams of two people each.

Each team member will need a sheet of paper, a pencil, and a calculator.

Setup

Each team member should turn his or her paper sideways (landscape orientation) and write the letters A through Z across the top.

Below the letters, write the numbers 1 through 26 as shown below.

A	B	C	D	E	F	G	…
1	2	3	4	5	6	7	…

Insecure Communications

As a team, you and your partner should decide on a prime integer (p) and an integer to use as your base (b). You should write these down.

You should not pick integers larger than 50 for either of these as it might make things too complicated.

Insecure Communications

This step simulates the insecure communications that take place as the conversation participants agree on a public key.

Key

Now each team member should select another integer (a) and keep it to himself.

Be careful not to pick an integer that is too large.

Key

Each team member should now perform the following calculation with his respective value of (a):

x = (b^a) mod p

p = prime, b = base, a = secret value

When you have completed this calculation, write down your respective value of x.

Key

For example, if you and your partner had decided on $p = 13$ and $b = 4$, and you selected 7 as your secret value a, you would get:

$$\begin{aligned} x &= (b \mathbin{\hat{}} a) \bmod p \\ &= (4 \mathbin{\hat{}} 7) \bmod 13 \\ &= (16384) \bmod 13 \\ &= 4 \end{aligned}$$

Key

Now you should swap values of x with your partner.

Perform the following calculation on your partner’s x-value:

$s = (x^b) \bmod p$

x = your partner’s value of x, b = base, p = prime

Key

For example, if my partner had given the value of 7 as her value of x, I would calculate:

$$\begin{aligned} s &= (x^b) \bmod p \\ &= (7^4) \bmod 13 \\ &= 2401 \bmod 13 \\ &= 9 \end{aligned}$$

Key

When you complete the calculation you should have an integer. Do not share this value with your partner. This will be the value of your key, which will correspond to the number of letters to rotate in the Caesar cipher.

Key

To find the shift value for ‘A’: Now take the value that you computed based on your partner’s x value (9 in the example calculation) and add 1 to it.

9 + 1 = 10

Now write the letter A under the space marked 10 on your sheet and continue to write the letters in order from left-to-right until you get to the end, then start back at the beginning.

Key

For example, you would end up with something like this:

…	G	H	I	J	K	L	M	…
…	7	8	9	10	11	12	13	…
…	X	Y	Z	A	B	C	D	…

Secure Communications

You and your partner may now communicate securely using the cipher key that you have agreed upon.

Secure Communications

To encrypt a message, write your original message on a sheet of paper, then underneath each letter, write the letter that appears below it on your cipher key. The bottom row of the message (the encrypted message) is what you will give to your partner.

Write and encrypt a short message and give it to your partner.

Secure Communications

To decrypt the message that your partner has just given you, find each letter in the encrypted message and replace it with the letter directly above on your cipher key.

When you have replaced every letter, you will have your decrypted message.

Secure Communications

If you have performed your calculations correctly, you and your partner should each be able to send encrypted messages and decrypt received messages using a key that you agreed upon securely over an insecure communication channel.

You have just successfully used the Diffie-Hellman key exchange algorithm in conjunction with a Caesar cipher to communicate securely.

Diffie-Hellman

In the real world, the values that you and your partner initially agreed upon would be much larger and you would use a better encryption algorithm than the Caesar cipher, but now you should understand how this algorithm works.