Diffie-Hellman

Based on *Cryptography Engineering* by Schneier, Ferguson, Kohno, Chapter 11

Lecture notes of Alexander Wood
awood@jjay.cuny.edu

John Jay College of Criminal Justice

Public-Key Cryptography

The field of cryptography was revitalised in 1976 when Whitfield Diffie and Martin Hellman published their paper “New Directions in Cryptography.”

Public-Key Cryptography

Up until this point all publicly known encryption systems were *private-key*, meaning the key had to be agreed upon and exchanged privately before encryption could take place.

Diffie and Hellman's paper introduced a method of **public-key encryption**, where a private key can be shared over an insecure channel.

Public-Key Cryptography

Diffie and Hellman posed the following question: Suppose you have an encryption algorithm where you public keys and private keys are different. Is it possible to publish your encryption key publicly while keeping your private key secret, enabling anyone to send you a secret message which only you can read?

Diffie-Hellman Key Exchange

They provided a partial solution to this problem called the **Diffie-Hellman Key Exchange Protocol**, or **DH protocol** for short.

Groups

This protocol is based off of some basic **group theory**. Let p be a large prime, 2000 to 4000 bits long. The DH protocol will operate within the group $\mathbb{Z}_p^*$ (the multiplicative group of integers modulo p).

Groups

Let g be a randomly chosen element in $\mathbb{Z}_p^*$. Denote this $g \in_R \mathbb{Z}_p^*$. Consider the infinite sequence

$$1, g, g^2, g^3, \ldots$$

Groups

Because we are working modulo p, the infinite sequence

$$1, g, g^2, g^3, \dots$$

can take only a finite number of values! In fact, at a certain point, the numbers in the sequence must start to repeat.

Groups

Let's consider a small example. Let $p = 211$, and let $g = 71$. Then the sequence

$$1, 71, 71^2, 71^3, \ldots$$

reduces modulo 211 to

$$1, 71, 188, 55, 107, 1, 71, 188, 55, 107, 1, \ldots$$

Groups

Let's go back to a general example. Let $1, g, g^2, g^3, \dots$ be a sequence for which $g^i = g^j$ for some $i < j$. Let's divide both sides by g^i! Then,

$$g^{j-i} = 1 \pmod{p}.$$

Order in Groups

We have therefore shown that there must exist some number q such that $g^q = 1 \pmod{p}$. Let the smallest positive value which satisfies this equation be called the **order** of g in $\mathbb{Z}_p^*$.

Order in Groups

For example, when $p = 211$, and let $g = 71$, the sequence

$$1, 71, 71^2, 71^3, \ldots$$

reduces modulo 211 to

$$1, 71, 188, 55, 107, \mathbf{1}, 71, 188, 55, 107, 1, \ldots$$

and hence the order of 71 modulo 211 is 5.

Generators

The sequence

$$1, g, g^2, g^3, \ldots, g^{q-1}$$

are the numbers we can reach in $\mathbb{Z}_p^*$ by exponentiating g. We say that g is a **generator** which **generates** the set $\{1, g, g^2, g^3, \ldots, g^{q-1}\}$ modulo p.

Primitive Elements

In $\mathbb{Z}_p^*$, there is at least one value g which generates the entire group! This means that there is a $g \in \mathbb{Z}_p^*$ such that $q = p - 1$. If g generates the entire group $\mathbb{Z}_p^*$ it is called a **primitive element** of $\mathbb{Z}_p^*$.

Important Fact

Theorem

For any $g \in \mathbb{Z}_p^*$, the order of g is a divisor of $p - 1$.

Important Fact

Theorem

For any $g \in \mathbb{Z}_p^*$, the order of g is a divisor of $p - 1$.

Proof.

Let g be a primitive element in $\mathbb{Z}_p^*$ and h any element. Since g generates $\mathbb{Z}_p^*$ there is some x, where $1 \leq x \leq p - 1$, such that $h = g^x$. The elements generated by h are $1, h, h^2, \ldots$, and can be written in terms of g as

$$1, g^x, g^{2x}, g^{3x}, \ldots.$$

(continued on next slide) □

Important Fact

Proof.

The order of h is the smallest q such that $h^q = 1$. This means that $g^{qx} = 1 \pmod{p}$. Note that $1 = g^0$. Because $g^{qx} = g^0 \pmod{p}$, we deduce that $qx = 0 \pmod{p-1}$ by Fermat's Little Theorem. This happens when

$$q = \frac{p-1}{gcd(x, p-1)}.$$

Therefore, q is a factor of $p-1$. □

Example

Let's look at our previous example where $p = 211$, and let $g = 71$, and $q = 5$. Note that

$$p - 1 = 210 = 2 \cdot 3 \cdot 5 \cdot 7$$

And q is, in fact, a factor of $p - 1$!

DH Protocol

Let p be a large prime and $g \in_R \mathbb{Z}_p^*$, where p and g are public.

1) Alice randomly chooses $x \in_R \mathbb{Z}_p^*$
2) Bob randomly chooses $y \in_R Z_p^*$
3) Alice sends $g^x \pmod{p}$ to Bob.
4) Bob sends $g^y \pmod{p}$ to Alice.

DH Protocol

Let p be a large prime and $g \in_R \mathbb{Z}_p^*$, where p and g are public.

1) Alice randomly chooses $x \in_R \mathbb{Z}_p^*$
2) Bob randomly chooses $y \in_R Z_p^*$
3) Alice sends $g^x \pmod{p}$ to Bob.
4) Bob sends $g^y \pmod{p}$ to Alice.
5) Alice computes $\kappa = (g^y)^x$
6) Bob computes $\kappa = (g^x)^y$

Diffie-Hellman Key Exchange

Public information: Large prime p, $g \in_R \mathbb{Z}_p^*$.

$$\begin{array}{lcl}
\textbf{Alice} & & \textbf{Bob} \\
x \in_R \mathbb{Z}_p^* & & y \in_R \mathbb{Z}_p^* \\
 & \xrightarrow{g^x \pmod{p}} & \\
 & \xleftarrow{g^y \pmod{p}} & \\
\kappa = g^{xy} \pmod{p} & & \kappa = g^{xy} \pmod{p}
\end{array}$$

The Diffie-Hellman Problem

Suppose Eve is eavesdropping on Alice and Bob's interactions. This means that she knows p, g, g^a, and g^b. She does *not* no a or b.

Finding the key reduces to the ability to reconstruct a from g^a.

The Discrete Log Problem

Finding x given g^x in real numbers is called computing logarithms. In $\mathbb{Z}_p^*$, we call this operation the **discrete logarithm.** The problem of computing x given g^x in $\mathbb{Z}_p^*$ is called the **discrete log problem** and is generally considered to be hard. ‘

Group Exercise

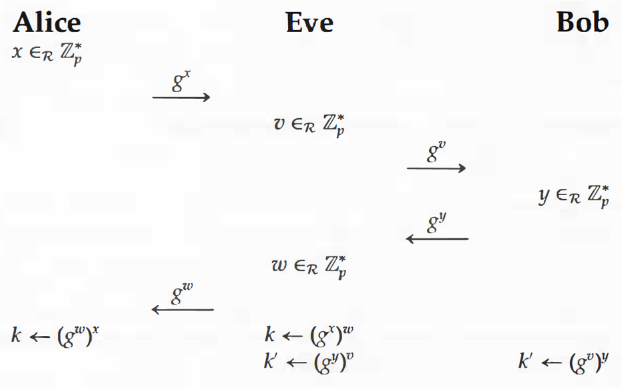
Let's test this out. Consider a prime number $p = 1918219$ and a randomly chosen generator of $\mathbb{Z}_p^*$, $g = 529$. Find a partner and carry out the following:

- Each partner privately picks a random number between 1 and p.
- Each partner privately computes $g^x \pmod{p}$ and shares it with the other partner
- Take the number your neighbor gave you, h, and compute h^x modulo p.
- Verify that you and your neighbor found the same value!
- Congratulations, you just carried out Diffie-Hellman (albeit with an absurdly small prime)

Man-In-The-Middle Attacks

This protocol does not protect against **Man in the Middle** attacks. Namely, Alice and Bob both are assuming that they are communicating with each other. What if, instead, a malicious third party Eve was intercepting and replacing the messages they send?

Man-In-The-Middle Attacks



Alice

$x \in_{\mathcal{R}} \mathbb{Z}_p^*$

$\xrightarrow{g^x}$

Eve

$v \in_{\mathcal{R}} \mathbb{Z}_p^*$

$\xrightarrow{g^v}$

Bob

$y \in_{\mathcal{R}} \mathbb{Z}_p^*$

$\xleftarrow{g^y}$

$w \in_{\mathcal{R}} \mathbb{Z}_p^*$

$\xleftarrow{g^w}$

$k \leftarrow (g^w)^x$

$k \leftarrow (g^x)^w$

$k' \leftarrow (g^y)^v$

$k' \leftarrow (g^v)^y$

Diagram from *Cryptography Engineering* by Schneier, Ferguson, Kohno

Digital Signatures

A **digital signature** can be used to protect against the Man-In-The-Middle attack, to be discussed later in the course.

Next Class

Next class we will discuss implementation of Diffie-Hellman.

References

- *Cryptography Engineering* by Schneier, Ferguson, Kohno, Chapter 11