To what extent can elliptic curves be used to establish a shared secret over an insecure channel?

Contents

Group Theory

Addition within the set of integers satisfy certain algebraic properties:

1. There exists an identity. For addition, 0 is the identity becuase $0 + a = a$.
2. The operation is associative, where $(a + b) + c = a + (b + c)$.
3. Every element has an inverse that is also within the set. For any $a \in \mathbb{Z}$, $-a$ is its inverse because $a + (-a) = 0$ where 0 is the identity element.
4. Closure. For any $a, b \in \mathbb{Z}$, we have $a + b \in \mathbb{Z}$ as well, therefore the operation will never output a value that leaves the $\mathbb{Z}$ set.

These four conditions satisfy the requirements for a *group*. We can say that the set of $\mathbb{Z}$ forms a group under addition. Note that $\mathbb{Z}$ does *not* form a group under multiplication, because although it satisfies three of the properties: 1 is the identity, the operation is associative, and for all $a, b \in \mathbb{Z}$, $ab \in \mathbb{Z}$ (closure), the inverse property is not satisfied.

For 2 to have an inverse, there would need to be $a \in \mathbb{Z}$ such that $2 \times a = 1$, the identity element. Such an a doesn't exist when a needs to be an integer.

However, we can restrict our set to make it form a group. Consider the numbers $\{1, 2, 3, .., n-1\}$ with multiplication modulo n, where n is a prime number. We will write this set as $\mathbb{Z}_n$.

For any $a \in \mathbb{Z}_n$, we have $1 \times a = a$, therefore 1 can be considered as the identity element. The operation is associative in the same way multiplication is associative, with the assumption that multiplying two numbers modulo n is equivalent to multiplying in $\mathbb{Z}$ then finding the result modulo n. Then, as $(ab)c = a(bc)$, we can say $(ab)c = a(bc) \pmod n$.

Finding an inverse for an element in $\mathbb{Z}_n$ requires the use of Fermat's Little Theorem, which states

$$a^{n-1} \equiv 1 \pmod n$$

when n is prime. Then, we can write $a \times a^{n-2} \equiv 1 \pmod n$. For any $a \in \mathbb{Z}_n$, a^{n-2} is its inverse as the product of a and a^{n-2} gives the identity. It's trivial to show that $\mathbb{Z}_n$ is closed under multiplication, therefore we can state that the set of non-zero integers modulo n forms a group under multiplication.

Introduction

Internet connections and data go through Internet Service Providers (ISP) which snoop on users' information. [citation needed] An often used method to prevent eavesdropping is through TLS, commonly known as the green padlock next to the address bar or HTTPS, [citation needed] which establishes a secure connection between the user and the website that they are connecting to, such that the ISP only knows which website they have connected to but does not know the content that the user has downloaded or uploaded.

TLS has many different cryptographic techniques to establishing a secure connection. One of which is the Elliptic Curve Diffie-Hellman (ECDH). In this paper, we will examine the mathematical theory underlying the ECDH operation and evaluate its practical application in cybersecurity.

The Discrete Log Problem in $\mathbb{Z}_p^\times$

As a consequence of Fermat's Little Theorem, we can write:

$$a^{p-1} \equiv 1 \pmod{p}$$
$$a \cdot a^{p-2} \equiv 1 \pmod{p}$$

For any integer a and prime p. We have found a^{p-2} as a's multiplicative inverse, therefore integers modulo p with multiplication forms a group, as the operation is associative, has an identity element, and every element has an inverse. This group is represented with the symbol $\mathbb{Z}_p^\times$.

Given a base 37 and a value 200, we can ask the following question:

$$17^n \equiv 24 \pmod{1009}$$

A method named pollard's ρ algorithm exists which we can use to find the answer. First, we generate random integers as exponents and write M:

$$M_1 = (17)^5(24)^{11}$$
$$M_2 = (17)^{20}(24)^7$$
$$M_3 = (17)^{13}(24)^6$$
$$M_4 = (17)^{11}(24)^{16}$$
$$M_5 = (17)^3(24)^{12}$$

Then, define

$$f(x) = xM_i \text{ if } x \equiv i \pmod{5}$$

This essentially gives a "random walk" of the group. Choose $P_0 = (17^3)(24^{14})$, then define

$$P_{n+1} = f(P_n)$$

We note that $P_{61} = P_{99} = 340$. If we kept track of the exponents on 17 and 24 in the calculations, we get

$$P_{61} = (17^{691})(24^{704}) = (17^{1075})(24^{1132}) = P_{99}$$

Then

$$17^{-384} = 24^{428}$$

Rewrite $24 = 17^k$

$$17^{-384} = 17^{428k}$$
$$17^{428k+384} = 1$$

Note that 17 has order 1008 in the multiplicative group modulo 1009, therefore we write

$$428k + 384 = 0 \pmod{1008}$$

(pollards rho, from Washington)

Given a and b are non-zero integers from this group, the discrete log problem asks us to find k such that

$$a^k \equiv b \pmod{p}$$

The assumption is that this problem is difficult to compute if the group and the exponent are well-chosen. This is used as the *trapdoor function* in cryptography, as it is assumed to be easy to compute in one direction and hard to compute in the other. We'll evaluate the extent to which this claim is true for $\mathbb{Z}_p^\times$ in later sections, but we'll start with this assumption.

Diffie-Hellman Key Exchange

When two people communicate through the Internet, they must do so through their internet service providers (ISPs). In the case of a public network, there may be malicious people pretending to be the router, thus making it so that your internet traffic goes through them. This is called a man-in-the-middle attack.

If the information being communicated is encrypted, then man-in-the-middle attacks would not work. Common encryption algorithms require the people involved to have a **shared secret**, for example a string of characters that only the two parties know. This is hard to do when the only form of communication is through an **insecure channel**, as in the case of internet connections. The Diffie-Hellman Key Exchange proposes a way to establish a shared secret even if the only channel to communicate in is insecure through the difficulty of the discrete log problem.

The mechanism is as follows:

Given a known base g in a group G (with exponentiation meaning repeated application of the group operation), Alice can establish a shared secret with Bob by generating secret integers. Alice can secretly generate a and send Bob g^a, while Bob can secretly generate b and send Alice g^b.

Alice can then compute $\left(g^b\right)^a$ and Bob can compute $\left(g^a\right)^b$. As both of these are equivalent to multiplying g to itself ab times, $\left(g^b\right)^a = \left(g^a\right)^b = g^{ab}$ can be used as the shared secret.

Because only g, g^a, and g^b are sent across the channel, any third party observer will not be able to compute g^{ab} without solving the discrete log problem to determine a or b. As we have assumed that the discrete log problem is difficult, this is a secure way for Alice to establish a shared secret with Bob if the only form of communication between the two is insecure.

Elliptic curves

Let an elliptic curve be denoted by the equation $y^2 = x^3 + Ax + B$ where A and B are constants. Note that the curve is symmetric about the x-axis, since if (x, y) is a point on the curve, $(x, -y)$ is also on the curve.

Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be distinct points on the curve, where $x_1 \neq x_2$. We can find a new point on the curve by defining a line that goes across the two points, with slope

$$m = \frac{y_2 - y_1}{x_2 - x_1}$$

And line equation

$$y = m(x - x_1) + y_1$$

We substitute this into the equation of the curve:

$$(m(x - x_1) + y_1)^2 = x^3 + Ax + B$$

Expanding and rearranging gives:

$$x^3 - m^2x^2 + (2m^2x_1 - 2y_1m + A)x + 2y_1mx_1 - m^2x_1^2 - y_1 = 0$$

With Vieta's formulas, the sum of roots for the cubic is m^2. We already know two roots of this polynomial as P_1 and P_2 are common points on the curve and the line, so we can find the x coordinate of the third point:

$$x_3 = m^2 - x_1 - x_2$$

In the group law, the y coordinate of the resulting point is flipped: (TODO: explain why)

$$y_3 = -(m(x_3 - x_1) + y_1) = m(x_1 - x_3) - y_1$$

Therefore, we have arrived at $P_3 = (x_3, y_3)$, a third point distinct from P_1 and P_2.

If only one point $P_1 = (x_1, y_1)$ is known, we can use implicit differentiation to find the tangent line:

$$y^2 = x^3 + Ax + B$$

$$2y\frac{\mathrm{d}y}{\mathrm{d}x} = 3x^2 + A$$

$$m = \frac{\mathrm{d}y}{\mathrm{d}x} = \frac{3x^2 + A}{2y} = \frac{3x_1^2 + A}{2y_1}$$

With the same line equation $y = m(x - x_1) + y_1$, with the same expanded formula:

$$x^3 - m^2x^2 + ... = 0$$

But this time, x_1 is a repeated root, as a tangent line either touches no other points at all (the case when $y = 0$) or touch one other point.

Therefore, we can find the third point with

$$x_3 = m^2 - 2x_1$$

And

$$y_3 = -(m(x_3 - x_1) + y_1) = m(x_1 - x_3) - y_1$$

Therefore, we can begin to define a group law for points on elliptic curves.

Let $C : y^2 = x^3 + Ax + B$ be the elliptic curve with the set of points that satisfy the given equation. We now show that $C \cup \{\infty\}$ forms a group.

Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be two points that are on the curve. Define $P_3 = P_1 + P_2$ to be as follows:

- If $P_1 = P_2 = (x_1, y_1)$, let

$$P_3 = (m^2 - 2x_1, m(x_1 - x_3) - y_1), \text{where } m = \frac{3x_1^2 + A}{2y_1}$$

- If $x_1 = x_2$ but $y_1 \neq y_2$ (N.B. the only case where this happens is $y_1 = -y_2$): let $P_3 = \infty$.
- Otherwise, let

$$P_3 = (m^2 - x_1 - x_2, m(x_1 - x_3) - y_1), \text{where } m = \frac{y_2 - y_1}{x_2 - x_1}$$

Additionally, define $P_1 + \infty = \infty + P_1 = P_1$, as well as $\infty + \infty = \infty$.

Proof that $C \cup \{\infty\}$ forms a group:

1. The operation $+$ is well-defined for any points $P_a + P_b$ where $P_a, P_b \in C \cup \{\infty\}$ as above.
2. ∞ is the identity element, where $P_a + \infty = P_a$ for all $P_a \in C \cup \{\infty\}$.
3. Every element has an inverse: let $P_a = (x, y)$, its inverse is $-P_a = (x, -y)$. TODO show that $-P_a \in C$.
4. The operation is associative, where $(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3)$. This is shown in chapter 2.4 in the book titled “Elliptic Curves: Number Theory and Cryptography”, and the proof gets too long, so we have omitted it here.