Introduction to Elliptic Curve Cryptography

June 26, 2024

1 Introduction

Elliptic curve cryptography uses the difficulty of solving the elliptic curve discrete logarithm problem in E, an elliptic curve, over the finite field $\mathbb{F}_p$, to provide better computational efficiency and smaller key sizes over traditional methods.

1.1 History

Elliptic Curve Cryptography was first proposed by Neal Koblitz in 1985 and Victor Miller independently in the same year. The idea gained popularity, especially after Lenstra's algorithm (1994) helped introduce elliptic curves to cryptography. Today, ECC is widely used in various applications, including secure web browsing (HTTPS), email encryption (PGP/GPG), and cryptocurrencies like Bitcoin.

1.2 Key Benefits

- Security: ECC is considered more secure than traditional RSA-based cryptography because it's resilient to quantum computer based attacks, whereas traditional algorithms like the RSA are not.
- Efficiency: ECC keys are generally shorter than RSA keys, making them faster and more efficient for encryption and decryption operations.
- Key sizes: ECC allows for smaller key sizes while maintaining equivalent security levels. For example, a 256-bit elliptic curve public key should provide comparable security to a 3072-bit RSA public key.

2 Prerequisites

2.1 Commutative Rings with Multiplicative Identity AKA Fields

Definition. A field is a commutative ring in which every nonzero element has a multiplicative inverse, where, a ring is a set R that has two operations, which we denote by $+$ and $\star$, having the following properties:

Properties of $+$

- Identity Law: There exists an additive identity $0 \in R$ such that $0 + a = a + 0 = a, \forall a \in R$.
- Inverse Law: $\forall a \in R, \exists b \in R, a + b = b + a = 0$, b is called the additive inverse.
- Associative Law: $a + (b + c) = (a + b) + c, \forall a, b, c \in R$
- Commutative Law: $a + b = b + a, \forall a, b \in R$

Properties of $\star$

- Identity Law: There is a multiplicative identity $1 \in R$ such that $1 \star a = a \star 1 = a, \forall a \in R$
- Associative Law: $a \star (b \star c) = (a \star b) \star c, \forall a, b, c \in R$
- Commutative Law: $a \star b = b \star a, \forall a, b \in R$

Property linking $+$ and $\star$

- Distributive Law: $a \star (b + c) = a \star b + a \star c$

Here are some examples of Rings and Fields you might already be familiar with.

- $R = \mathbb{Q}, \star = \times$, addition as usual. The multiplicative identity element is 1. Every nonzero element has a multiplicative inverse, so $\mathbb{Q}$ is a field.
- $R = \mathbb{Z}, \star = \times$, and addition as usual. The multiplicative identity element is 1. The only elements that have multiplicative inverses are 1 and -1, so $\mathbb{Z}$ is a ring, but it is not a field.
- More generally, if R is any ring, we can form a ring of polynomials whose coefficients are taken from the ring R. We will discuss these general polynomial rings later.

2.2 Quotient Rings and Divisibility

The concept of divisibility can be generalized to any ring.

Definiton. Let R be a ring. An element $u \in R$ is called a unit if it has a multiplicative inverse. An element a of a ring R is said to be irreducible if a is not a unit and if in every factorization of a is $a = b \star c$, either b is a unit or c is a unit.

The integers have the property that every integer factors uniquely into a product of irreducible integers (primes). Not every ring has this important unique factorization property, but in the next section we see that the ring of polynomials with coefficients in a field is a unique factorization ring. Using the definition of divisibility, we can extend the notion of congruence to arbitrary rings.

For every ring R, let $m \in R, m \neq 0$. If

$$a_1 \equiv a_2 \pmod{m} \tag{1}$$
$$b_1 \equiv b_2 \pmod{m} \tag{2}$$

Then

$$a_1 + b_1 \equiv a_2 + b_2 \pmod{m} \tag{3}$$
$$a_1 \star b_1 \equiv a_2 \star b_2 \pmod{m} \tag{4}$$

This shows a method to create new rings from old rings, just as we created $\mathbb{Z}/q\mathbb{Z}$ from $\mathbb{Z}$ by looking at congruences modulo q.

Definition. Let R be a ring and let $m \in R$ with $m \neq 0$. For any $a \in R$ we write $\overline{a}$ for the set of all $a' \in R$ such that $a' \equiv a \pmod{m}$. This set is called the congruence class of a, and we can denote the collection of all congruence classes by $R/mR = \{\overline{a} : a \in R\}$.

2.3 Polynomial Rings

If R is any ring, then we can create a polynomial ring with coefficients taken from R. This ring is denoted by

$$R[x] = \{a_0 + a_1x + a_2x^2 + \cdots + a_nx^n : n \geq 0, a_i \in R\} \tag{5}$$

The degree of the polynomial is the exponent of the highest power of x that appears. We denote the degree of any polynomial $a(x)$ by $\deg(a)$, and we call a_n the leading coefficient of $a(x)$. A nonzero polynomial whose leading coefficient is equal to 1 is called a monic polynomial.

We can perform polynomial long division on any polynomial ring $\mathbb{F}[x]$ as long as $\mathbb{F}$ is a field. Rings of these ”division with remainder” algorithm are called Euclidean rings.

2.4 Quotients of Polynomial Rings and Finite Fields of Prime Order Power

We combine polynomial rings and quotient rings, and start to consider quotients of polynomial rings in a finite field.

Let $\mathbb{F}$ be a field and let $m \in \mathbb{F}[x]$ be a nonzero polynomial. Then every nonzero congruence class $\overline{a} \in \mathbb{F}[x]/(m)$ has a unique representative r satisfying,

$$\deg r < \deg m \tag{6}$$
$$a \equiv r \pmod{m} \tag{7}$$

Consider the ring $\mathbb{F}[x]/(x^2+1)$, then every element of this quotient ring has the form

$$\overline{\alpha+\beta x} \quad \alpha, \beta \in \mathbb{F} \tag{8}$$

Addition is performed as expected,

$$\overline{\alpha_1+\beta_1 x}+\overline{\alpha_2+\beta_2 x}=\overline{(\alpha_1+\alpha_2)+(\beta_1+\beta_2)x} \tag{9}$$

Multiplication is also similar, just that we need to reduce the polynomial by x^2+1 and take the remainder

$$\begin{align} \overline{\alpha_1+\beta_1 x}\cdot\overline{\alpha_2+\beta_2 x} &= \overline{\alpha_1\alpha_2+(\alpha_1\beta_2+\alpha_2\beta_1)x+\beta_1\beta_2 x^2} \tag{10} \\ &= \overline{(\alpha_1\alpha_2-beta_1\beta_2)+(\alpha_1\beta_2+\alpha_2\beta_1)x} \tag{11} \end{align}$$

The effect of dividing by x^2+1 is the same as replacing x^2 with -1. The intuition is that since we are taking $\mathbb{F}[x]/(x^2+1)$, we have made the quantity $x^2+1=0$.

Let $\mathbb{F}_p$ be a finite field and let $m \in \mathbb{F}_p[x]$ be a nonzero polynomial of degree $d \geq 1$. Then the quotient ring $\mathbb{F}_p[x]/(m)$ contains exactly p^d elements. To show this we just need to count the possible values each coefficient of x^d where $0 \leq n \leq d-1$.

Let $\mathbb{F}_p$ be a finite field and let $a, m \in \mathbb{F}_p[x]$ be polynomials with $m \neq 0$. Then $\overline{a}$ is a unit in the quotient ring $\mathbb{F}[x]/(m)$ if and only if $\gcd(a,m)=1$. This also implies that a has an inverse. Which also implies that the quotient ring $\mathbb{F}[x]/m$ is a field.

Let $\mathbb{F}$ be a finite field having q elements. Then $\mathbb{F}$ has a primitive root. There is an element $g \in \mathbb{F}$ such that

$$\mathbb{F}^* = \{1, g, g^2, g^3, \ldots, g^{q-2}\} \tag{12}$$

2.5 The Discrete Logarithm Problem

The discrete logarithm problem is considered a solution to the one-way trapdoor function. A one-way function is an *invertible* that is is easy to compute, but whose inverse is difficult to compute, unless you know the trapdoor information. Well how hard is hard? Intuitively, a function is difficult to compute if any algorithm that attempts to compute the inverse in a ”reasonable” amount of time, i.e, the age of the universe, will almost certainly fail. Here ”almost certainly” is defined probabilistically.

Primitive Root Theorem: Let p be a prime number. Then there exists an element $g \in \mathbb{F}_p^*$ having order $p-1$.

$$\mathbb{F}_p^* = \{1, g, g^2, g^3, ..., g^{p-2}\} \tag{13}$$

Elements with this property are called primitive roots of $\mathbb{F}_p$, or generators of $\mathbb{F}_p^*$. They are the elements of $\mathbb{F}_p^*$ having order $p-1$. The proof of this can be googled should the reader require a rigorous approach to understanding.

Definition. Let g be a primitive root for $\mathbb{F}_p$, and let h be a nonzero element of $\mathbb{F}_p$. The Discrete Logarithm Problem (DLP) is the problem of finding an exponent x such that:

$$g^x \equiv h \pmod{p} \tag{14}$$

The number x is called the discrete logarithm of h to the base g and is denoted by $\log_g(h)$

The discrete logarithm problem is a well poised one, find the integer x. However if there is one such solution, there are infinitely many, because by Fermat's little theorem, $g^{p-1} \equiv 1 \pmod{p}$, this implies that,

$$g^{x+k(p-1)} = g^x \cdot (g^{p-1})^k \equiv h \cdot 1^k \equiv h \pmod{p} \tag{15}$$

One could say that $\log_g$ gives a well-defined function

$$\log_g : \mathbb{F}_p^* \to \frac{\mathbb{Z}}{(p-1)\mathbb{Z}} \tag{16}$$

As an example, consider $g = 2, h = 10, p = 11$

$$2^x \equiv 10 \pmod{11}$$

One can easily verify that $x = \log_2(10) = 5$. Now we can define the discrete logarithm problem generally for any group, G.

Definiton. Let G be a group whose group law we denote by the symbol $\star$. The discrete logarithm problem for G is to determine, for any two given elements g and h in G, an integer x satisfying

$$\underbrace{g \star g \star g \star g \cdots \star g}_{x \text{ times}} = h \tag{17}$$