p-adic Cryptography

Grace Howard

August 2022

1 Cryptography

Definition 1.1. *Plaintext* is text which has not yet been encrypted, or has already been decrypted.

Definition 1.2. *Ciphertext* is text which has been encrypted using an algorithm.

Let P denote plaintext and let C denote ciphertext. By going from plaintext to ciphertext, the message has been encrypted, and by going from ciphertext to plaintext the message has been deciphered. Additionally, there are characters which are defined to be any letter a-z, punctuation, symbols, numbers, and blanks. Let f denote an enciphering transformation such that

$$P \xrightarrow{f} C.$$

Then, f^{-1} is the *deciphering* transformation used to decipher the text, or

$$C \xrightarrow{f^{-1}} P.$$

With this, a *cryptosystem* is an arrangement such that

$$P \xrightarrow{f} C \xrightarrow{f^{-1}} P.$$

Here, assume f has a one-to-one correspondence.

2 Keys

Definition 2.1. A *key* K can be used to encode and decode data. It is typically a string of letters or numbers, which are passed through an algorithm to obtain the desired data.

3 Elliptic Functions

Definition 3.1. An *elliptic function* is a doubly periodic function. In other words, for ω_1, ω_2,

$$f(z+\omega_1) = f(z)$$

$$f(z+\omega_2) = f(z)$$

for all $z \in \mathbb{C}$. It is also a meromorphic function, meaning it has no singularities, or points at which the function is undefined, except for poles.

3.1

For example, the Weierstrass $\wp$ function

$$\wp(z;\Lambda) = \frac{1}{z^2} + \sum_{w \in \Lambda *} \frac{1}{(z-w)^2} - \frac{1}{w^2},$$

where $\Lambda \subset \mathbb{C}$, and $\Lambda *$ is $\Lambda - \{0\}$

and its derivative

$$\wp'(z;\Lambda) = -2 \sum_{w \in \Lambda *} \frac{1}{(z-w)^3}$$

are elliptic functions.

Weierstrass elliptic functions, or $\wp$- functions, can be used with their derivatives to parameterize an elliptic curve.

4 Elliptic Curves

An *elliptic curve* over a field F is a set of (x,y) in F^2 which satisfy an equation of the form

$$y^2 = x^3 + ax + b$$

where $a, b \in F$ with the point at infinity I. They can be put into an algebraic form with the use of a Weierstrass elliptic function.

For example,

$$y^2 = x^3 - 1$$

is cubic with no repeating roots.
Let

$$x = \frac{X}{Z}$$

and

$$y = \frac{Y}{Z}.$$

Then,

$$y^2 = x^3 - 1 = \left(\frac{Y}{Z}\right)^2 = \left(\frac{X}{Z}\right)^3 - 1$$

Taking $\left(\frac{Y}{Z}\right)^2 = \left(\frac{X}{Z}\right)^3 - 1$,

$$(Z^3)\frac{Y^2}{Z^2} = \frac{X^3}{Z^3} - 1(Z^3)$$

$$= Y^2Z = X^3 - Z^3.$$

Then, if (X, Y, Z) is a solution, $(\alpha X, \alpha Y, \alpha Z)$ is also for all α .

Let $X = 0$ and $Z = 0$ and let $Y \neq 0$. Then,

$$(0 : Y : 0) = (0 : 1 : 0),$$

which is a point on the projective curve, but not in the Cartesian plane. This point is the point at infinity.

5 Elliptic Curve Cryptography

Definition 5.1. *Elliptic Curve Cryptography* employs the use of cryptosystems based on the structure of elliptic curves.

5.1 Elliptic Curves over Finite Fields

Let $\mathbb{F}_q$ be a finite field with q elements. Let E be an elliptic curve defined over $\mathbb{F}_q$. Then the number of rational points of E is

$$|\#E(K) - (q + 1)| \leq 2\sqrt{q}.$$

5.2 Elliptic Curves over p-adic Fields

Let E be an elliptic curve over $\mathbb{Q}_p$. Then the group of points on E (which are p-adic) is given by

$$E(\mathbb{Q}_p) = \{[a : b : c] \in P^2(\mathbb{Q}_p) : F(a, b, c) = 0\}$$

where $P^2(\mathbb{Q}_p)$ is the projective plane over $\mathbb{Q}_p$ and F is from $E = Z(F)$.

6 Public Key Cryptography

Definition 6.1. *Public key*, or *Asymmetric* cryptography utilizes a pair of keys, one of which is the public key.

A public key may be, as the name infers, public. The other of which is the private key, which is kept private. It relies on the difficulty of some problems in math. Namely, the discrete logarithm problem.

Key Exchange

Symmetric encryption requires the sender and receiver of information to be using the same key when encrypting and decrypting data. Asymmetric encryption uses different keys for encrypting and decrypting data.

First, a pair of keys are generated. One of these is the private key and the other is the public key. Then, public keys are exchanged. Following this, the data is encrypted using the public key of the receiver. The data is then transmitted. Finally, the receiver decrypts the message using their private key.

7 Discrete Logarithm Problem

Let $\mathbb{F}_p^\times$ denote the group of nonzero elements in $\mathbb{F}_p$ with the operation of multiplication. Given a prime p and a primitive root r, the discrete logarithm of y, where $y \in \mathbb{F}_p^\times$, with respect to r is the $x \in \mathbb{Z}$ such that

$$r^x = y$$

where $1 \leq x \leq p - 1$.

Elliptic Curve Discrete Logarithm Problem

Let E be an elliptic curve over $\mathbb{F}_q$, and let B be a point of E, then given a point $P \in E$, the goal is to find $x \in \mathbb{Z}$ such that

$$xB = P$$

if x exists.

8 Diffie- Hellman Key Exchange

Definition 8.1. A *key exchange* exchanges information securely over a private channel. With the use of a private key, the protocol allows for secure communication even with the intervention of an unwanted monitor.

Let q be known so the finite field $\mathbb{F}_q$ of the key will be known. Suppose an element g is also known and is a generator of $\mathbb{F}_q^*$. Then suppose A selects an integer a where $1 < a < q-1$ and calculates $g^a \in \mathbb{F}_q$. The integer a is kept secret, while g^a is made public. Then B selects an integer b where $1 < b < q-1$ and calculates $g^b \in \mathbb{F}_q$. Similarly, b is kept secret and g^b is made public. Then, the *secret key* is g^{ab}. Since B knows g^a as well as b and A knows g^b as well as a, either can compute the key g^{ab}.

9 Pohlig- Hellman Algorithm

The Pohlig- Hellman Algorithm assists in solving the Discrete Logarithm Problem. Let p be a prime. Let α denote a primitive element in $\mathbb{Z}_p$,and let $\beta \in \mathbb{Z}_p^*$. Then the goal is to find

$$a = log_\alpha \beta$$

where $0 \leq a \leq p-2$. Then,

$$p - 1 = p_1^{c_1} p_2^{c_2} p_3^{c_3} ... p_n^{c_n}.$$

Let $x = a \bmod p_i^{c_i}$. Then,

$$x = \sum_{i=0}^{c_i-1} a_i p_i^i$$

where $0 \leq a_i \leq p_i - 1$. Using this,

$$a = a_0 + a_1 p_i + \cdots + a_{c_i-1} p_i^{c_i-1} + d p_i^{c_i}$$

for an integer d. So, a_0 can be determined using

$$\beta \frac{p-1}{p_i} \equiv \alpha \frac{a_0(p-1)}{p_i} \bmod p.$$

Then, $a_1, ..., a_{c_i-1}$ can be found. Let

$$\beta_j = \beta_0 \alpha^{-(a_0 + a_1 p_i + ... + a_{j-1} p_i^{j-1})} \bmod p$$

for $0 \leq j \leq c_i - 1$. With this,

$$(\beta_j) \frac{p-1}{p_i^{j+1}} \equiv \alpha \frac{a_j(p-1)}{p_i} \bmod p.$$

Noting

$$\beta_{j+1} = \beta_j \alpha^{-(a_j p_i^j)} \bmod p,$$

$a_0, \beta_1, a_1, ..., \beta_{c_i-1}, a_{c_i-1}$ can be found.