16 Discrete Logarithm Problem

The **Discrete Logarithm Problem** (DLP) is a fundamental mathematical problem in cryptography.

16.1 Definition of the Discrete Logarithm Problem

Let p be a large prime, there exists a **primitive root** g in the field $\mathbb{F}_p$. This means that every nonzero element of $\mathbb{F}_p$ can be written as some power of g.

In particular, by Fermat's Little Theorem:

$$g^{p-1} \equiv 1 \pmod{p}$$

and no smaller positive power of g is congruent to 1. Thus, the elements of the multiplicative group $\mathbb{F}_p$ are:

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

Definition of the Discrete Logarithm Problem (DLP)

Definition 16.1. Let g be a primitive root of $\mathbb{F}_p$, and let h be a nonzero element of $\mathbb{F}_p$. The **Discrete Logarithm Problem** is the problem of finding an exponent x such that:

$$g^x \equiv h \pmod{p}.$$

The number x is called the **discrete logarithm** of h to the base g and is denoted by:

$$\log_g(h).$$

16.2 Applications in Cryptography

The Discrete Logarithm Problem forms the basis for several cryptographic protocols, include **Diffie-Hellman Key Exchange**, **ElGamal Encryption** and **Digital Signature Algorithms**