How to Change the World with Donald Knuth

Abraham Xiao

Masdar Institute of Science and Technology

Information Security Project Presentation

Discrete Logarithm in a Nutshell

The security of many cryptographic techniques depends on the intractability of discrete logarithm problem.

A partial list of these include:

- DiffieHellman key agreement and its derivatives.
- ElGamal encryption.
- ElGamal signature scheme and its variants.

General setting for algorithms in this section are:

- A (multiplicatively written) finite cyclic group G
- n is the order of group G
- α is a generator of group G[1]

[1] For more math background, refer to [Ros12].

Relevant Definitions

Cyclic group and its generator.

Definition

A group is *cyclic* if there is an element $\alpha \in G$ such that for each $b \in G$ there is an integer i with $b = \alpha^i$. Such an element α is called a generator of G.

Discrete logarithm.

Definition

Let G be a finite cyclic group of order n. Let α be a generator of G, and let $\beta \in G$. The *discrete logarithm of* β *to the base* α, denoted $\log_\alpha \beta$, is the unique integer x, $0 \leq x \leq n-1$, such that $\beta = \alpha^x$[MVO96].

A Discrete Logarithm Example

Example

Let $p = 97$. Then $\mathbb{Z}_{97}^*$ is a cyclic group of order $n = 96$. A generator of $\mathbb{Z}_{97}^*$ is $\alpha = 5$. Since $5^{32} \equiv 35 \mod 97$, $\log_5 35 = 32$ in $\mathbb{Z}_{97}^*$.

The DiffieHellman Problem

The DiffieHellman problem is closely related to the well-studied discrete logarithm problem.

Definition

The *DiffieHellman problem* is the following: given a prime p, a generator α of $\mathbb{Z}_p^*$, and elements $\alpha^a \mod p$ and $\alpha^b \mod p$, find $\alpha^{ab} \mod p$.

Wait! Could we just possibly do

$$\alpha^a \times \alpha^b \rightarrow \alpha^{ab} \tag{1}$$

Well, life is not as easy as it looks like...

$$\alpha^a \times \alpha^b = \alpha^{a+b} \tag{2}$$

Links between Discrete Logarithm and DiffieHellman Problem

Suppose that the discrete logarithm problem in $\mathbb{Z}_p^*$ could be efficiently solved[2]. Then given α, p, $\alpha^a \mod p$ and $\alpha^b \mod p$, one could first find a from α, p and $\alpha^a \mod p$ by what?!

Solving a discrete logarithm problem, and then compute $(\alpha^b)^a = \alpha^{ab} \mod p$.

[2]In math, the assumption is as important as,
if not more important than induction in many situations.

ElGamal public-key encryption

The ElGamal public-key encryption scheme can be viewed as DiffieHellman key agreement[3] in key transfer mode.
Its security is based on the intractability of the discrete logarithm problem (Section 1) and the DiffieHellman problem (Section 2).

[3] Yet another fancy nickname for key exchange

Ensure: A public key and its corresponding private key is created for every entity.

Steps to generate key pairs are described as follows:

1. Generate a prime p that is large enough and cannot be predicted, i.e. it should be generated randomly. Find a generator α of the multiplicative group $\mathbb{Z}_p^*$ of integers modulo p.
2. Randomly select an integer a satisfying $1 \leq a \leq p-2$. Then calculate $\alpha^a \mod p$.
3. The public key is returned as (p, α, α^a); The private key is returned as a.

Figure : **Algorithm** Key generation for ElGamal public-key encryption

References I

- Alfred J. Menezes, Scott A. Vanstone, and Paul C. Van Oorschot, *Handbook of applied cryptography*, 1st ed., CRC Press, Inc., Boca Raton, FL, USA, 1996.
- Kenneth H. Rosen, *Discrete mathematics and its applications*, 7th ed., McGraw-Hill Higher Education, 2012.