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.

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].

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.