
1 Diffie-Hellman and El Gamal

Dario Köllner ...

Abstract

Introduction

Here comes the intro....

1.1 Diffie-Hellmann Security

1.1.1 Computational-Diffie-Hellman-Problem

The Computational-Diffie-Hellman-Problem relies on the mathematical discrete logarithm problem, which is used in more than one encryption protocol.

Definition 1. Let G a finite cyclic group of the order p . If p is a prime number and g a primitive root mod p then for every $A \in \{1, 2, \dots, p-1\}$ there is exactly one exponent $a \in \{0, 1, 2, \dots, p-2\}$ with $A \equiv g^a \pmod{p}$ [1].

Which means „the exponent a is called *discrete logarithm* of A to the basis of g “ [1]. Currently there is no suitable algorithm for an efficient calculation for this mathematical problem known. The cumulative distribution function of the discrete logarithm appears to be very random for a big prime group. This leads to the fact, that the discrete logarithm can not be calculated in a sufficient time for attackers.

1.1.2 Decisional-Diffie-Hellman-Problem

1.1.3 Primenumbers p and Bitlength q

1.1.4 Man in the middle attack

1.2 El Gamal problems

1.2.1 Protocol problems

1.2.2 Subgroup problems

Literatur

- [1] Johannes Buchmann. *Einführung in die Kryptographie*. 6., überarbeitete Auflage. Springer-Lehrbuch. Berlin und Heidelberg: Springer Spektrum, 2016.
ISBN: 978-3-642-39775-2. DOI: [10.1007/978-3-642-39775-2](https://doi.org/10.1007/978-3-642-39775-2).
URL: <http://www.lehmanns.de/midvox/bib/9783642397745>.