1 Diffie-Hellman and El Gamal

Dario Köllner ...

Abstract

Introduction

Here comes the intro....

1.1 Diffie-Helmann Security

1.1.1 Computational-Diffie-Hellman-Problem

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

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 $A \in \{1, 2, ..., p-1\}$ there is exactly one exponent $a \in \{0, 1, 2, ..., p-2\}$ with $A \equiv g^a \mod n$ [1][2].

Which menas „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 mathmatical 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 calculated in a sufficient time for attackers.

When an attacker gets the numbers *p*, *g*, *A* and *B* he does not know the discrete logarithm. He has to calculate the secret key. So in fact the Computational-Diffie-Hellman-Problem is to calculate the secret key $K = g^{ab} \mod p$ [1][2][3].

1.1.2 Decisional-Diffie-Hellman-Problem

1.1.3 Primenumber p and Bitlength q

1.1.4 Man in the middle attack

Another attack on the Diffie-Hellman is the Man-In-The-Middle-Attack. This attack is quite common and can be used in a lot of situaitons. The attack infiltrates the communication between two instances Alice (A) and Bob (B). This makes it possible to influence the communication in a bad way. The attacker Mallory (M), the instance between A and B can spoofe and simulate towards A to be B and the other way round (see figure 1).

In case of the Diffie-Hellman protocoll it means that Alice sends $g^a \mod p$ to Mallory instead of Bob. Mallory sends now $g^m \mod p$ with the own parameter *m* to Bob and simulates over Bob to be Alice. For Bob it appears that Alice sent the request and sends $g^b \mod p$ back. Now M sends

$g^b \mod p$ back to Alice. The secret key pair for A and M are $K_A = g^{am} \mod p$ and $K_{AM} = g^{am} \mod p$. For M and B the pair looks like this: $K_{BM} = g^{bm} \mod p$ and $K_B = g^{bm} \mod p$.

Mallory can now decrypt and encrypt every message that A and B sending each other and listens the communication.

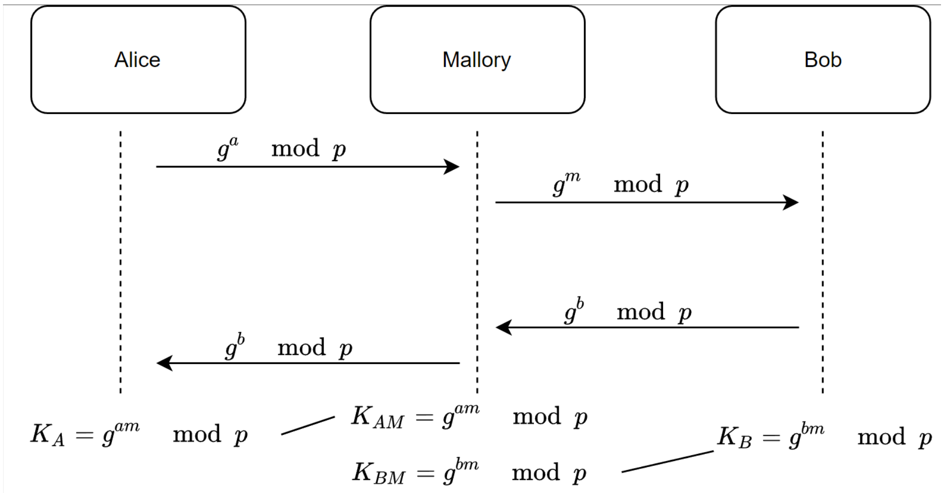

Figure 1: Man in the middle diagram

1.2 El Gamal problems

1.2.1 Protocol problems

1.2.2 Subgroup problems

References

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

[2] Nigel Smart. *Cryptography Made Simple*. Information Security and Cryptography. Cham: Springer International Publishing, 2015. ISBN: 978-3-319-21936-3. URL: http://nbn-resolving.org/urn:nbn:de:bsz:31-epflicht-1603383.

[3] *Sichere Netzwerkkommunikation: Grundlagen, Protokolle und Architekturen ; mit 12 Tabellen*. X.systems.press. Berlin and Heidelberg: Springer, 2005. ISBN: 3-540-21845-9.