
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][2].

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.

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 $K = g^{ab} \pmod{p}$ [1][2][3].

1.1.2 Decisional-Diffie-Hellman-Problem

1.1.3 Primenumbers p and Bitlength q

As conclusion of the Computational- and Decisional-Diffie-Hellman-Problem it is now known that the logarithm modulo p is not efficient. But only if the group G is big enough, which means the primenumber p must be also really big. Another security improvement is to increase the bitlength of q . Currently a good amount would be around 3000 bit [1]. As in the table 1 is shown the recommended bitlength for q in the future is 512 and a minimum size p of 15,424. These numbers are necessary due to the increasing calculation power of the hardware. The 512 bit length for different usages is nowadays common and standard, besides 256 bit.

Proctection till	Minimum size p	Bitlength q
2015	1248	160
2020	1776	192
2030	2432	224
2040	3248	256
Future	15,424	512

Table 1: Primenumber p and Bitlength q length estimation [1]

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 situations. 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 spoof and simulate towards A to be B and the other way round (see figure 1).

In case of the Diffie-Hellman protocol it means that Alice sends $g^a \bmod p$ to Mallory instead of Bob. Mallory sends now $g^m \bmod p$ 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 $g^b \bmod p$ back. Now M sends $g^b \bmod p$ back to Alice. The secret key pair for A and M are $K_A = g^{am} \bmod p$ and $K_{AM} = g^{am} \bmod p$. For M and B the pair looks like this: $K_{BM} = g^{bm} \bmod p$ and $K_B = g^{bm} \bmod p$.

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

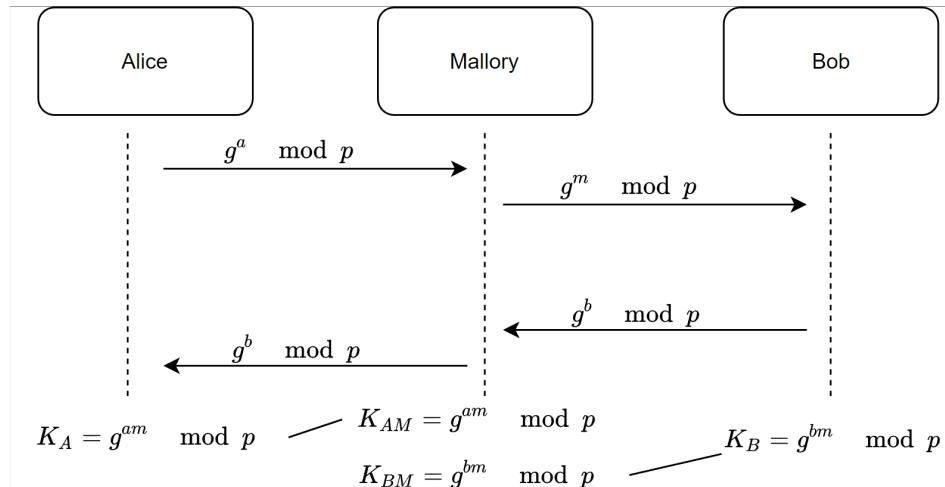


Figure 1: Man in the middle diagram

1.2 El Gamal problems

1.2.1 Protocol problems

Even though the ElGamal-Protocol is considered as safe this is only true when following the exact protocol. As explanation for the statement a look at random number r will show it. If r is used on more than one message the messages will be unsecure. This is because the exponentiation of the group has to be calculated just once. This takes also affect when seeing through the perspective of an attacker. Even though he does not know the number r the attacker can recognize a specific pattern and conclude to r and break the encryption.

1.2.2 Subgroup problems

Another problem is the same as in the Diffie-Hellman-Protocoll with the subgroups [1][3][2]. Let define that q of \mathbb{G} is a prime number, then the trivial group is the only subgroup of \mathbb{G} . Then for every n in q , there is a subgroup \mathbb{G} with the order n . To identify if it is a element of the subgroup just proof if $h^n = 1$ [1][3][2]. Therefore attacks are possible. The solution is a enough big subgroup to resist the attack which means the prime number has to be really big.

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](https://doi.org/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.