Secure Communication Protocols

Abstract

In this assignment, we implement a secure communication protocol consisting of three consecutive steps. First, we use Diffie-Hellman[1] key exchange to craft a shared private key between two actors using public key cryptography. We then use an implementation of the Blum Blum Shub[1] algorithm to generate a cryptographically secure pseudo-random shared private key, using the previously exchanged key as seed. Finally, we use the generated random key to encrypt and decrypt messages between the two actors using 128-bit AES ciphers.

1 Introduction

Our main goal is to be able to communicate secret data over an unsecure communication channel. To do so, we have to encrypt our data before sending it, and decrypt it after recieving it, so that it only appears encrypted on the communication channel. To perform these encryptions, we want to use a symmetric cipher allowing us to efficiently compute ciphertext from plaintext and vice versa. Before using symmetric encryption, we have to solve the key exchange problem, because we still need to communicate the private key between the two actors over an unsecure channel. One answer to this first problem is to use public-key cryptography, and most specifically the Diffie-Hellman key exchange protocol.

1.1 Diffie-Hellman

This key exchange scheme allows us to create a shared private key by only communicating public data. It relies on the computational difficulty of computing discrete logarithms. It has been formulated in 1976 by Whitfield Diffie and Martin Hellman. We use it to generate a first shared private key between two actors, Alice and Bob.

1.2 Blum Blum Shub

To increase the strength of the exchanged key, we use it as a seed to a cryptographically strong pseudo-random number generator. The chosen stream generator is Blum Blum Shub, which outputs the least significant bit of x_{n+1} at each step of the following sequence.

$$x_{n+1} = x_n^2 \bmod M \qquad \text{with } x_0 = \text{seed}, M \text{ the product of two large primes } p \text{ and } q$$

1.3 Advanced Encryption Standard

To encrypt their messages, Alice and Bob can now use a symmetric cipher with their shared private key. Here, we use AES in Electronic Code Book mode, so that we do not have to send nonces and tags. Now that Alice and Bob exchanged their keys, they could use any symmetric cipher and mode of operation. We only use this mode because the cipher implementation is not part of this assignment, so we keep it simple.

2 Design and Implementation

2.1 Diffie-Hellman

Talk about group used. (https://www.rfc-editor.org/rfc/rfc5114.html) Naive exponentiation vs pow ! 10^{616}

2.2 Blum Blum Shub

2.3 Advanced Encryption Standard

3 Test Results

4 Discussion

Blum blum shub is slow and not practically secure (https://crypto.stackexchange.com/questions/3454/blum-blum-shub-vs-aes-ctr-or-other-csprngs)

5 Conclusion

References

[1] William Stallings. *Cryptography and network security: principles and practice.* Pearson, 2017.