Secure Communication Protocols

Abstract

In this assignment, we implement a secure communication protocol consisting of three consecutive steps. First, we use Diffie-Hellman 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 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

2 Design and Implementation

3 Test Results

4 Discussion

5 Conclusion