TAMPERE UNIVERSITY – DEPARTMENT OF COMPUTING SCIENCES

Security Protocols: Helping Alice and Bob to Share Secrets (COMP.SEC.220)

Tutorial 4: Security Protocols

Antonis Michalas antonios.michalas@tuni.fi
Mindaugas Budzys mindaugas.budzys@tuni.fi
Hossein Abdinasibfar hossein.abdinasibfar@tuni.fi

August 19, 2024

SUBMISSION DEADLINE: 30.09.2024 AT 23:00

Tutorial Description

During lectures 4 and 5, you were introduced to security protocols and authentication techniques. In this tutorial, you will be tasked with implementing the Diffie-Hellman Key Exchange protocol. The purpose of this tutorial is to help you better understand how the Diffie-Hellman key exchange protocol works and how security protocols work in general. To this end, you will not only have the opportunity to implement the actual protocol but also to examine its security and its use in practice.

EXERCISE 1 – DIFFIE-HELLMAN KEY EXCHANGE

TASK 1: Alice and Bob exchange a shift cipher key using the DH key exchange. They agree to use the prime number $p = 19$ for their cyclic group $\mathbb{Z}_{19}^*$ and $g = 3$ as the generator.
Assume Alice uses the secret value $a = 7$ and Bob the secret value $b = 5$. Compute the intermediate values and the final key that Alice and Bob exchange.

TASK 2: Alice and Bob exchanged a secret key for a shift cipher encryption scheme by using DH with the following parameters:

- $g = 5$ and
- $p = 47$.

The numbers exchanged were $X = 99$ and $Y = 23$. Can you find the key that Alice and Bob agreed upon?

TASK 3: Using the key computed in task 2, decrypt the message: "Rxu rqob vhfxulwb lv rxu delolwb wr fkdqjh -Mrkq Oloob". What is the decrypted message?

EXERCISE 2 – DIFFIE-HELLMAN EXTENSION

Design a protocol that allows three friends Alice (A), Bob (B) and Charlie (C) to exchange a single symmetric key K, minimizing the number of exchanged messages. To do this, you will need to extend the DH key exchange protocol.

Your solution must satisfy the following conditions:

1. Only A, B and C should get access to the key K;
2. The integrity of the exchanged key should be properly verified by all the recipients;
3. Use as few messages as possible.

EXERCISE 3 – DIFFIE-HELLMAN IMPLEMENTATION

Implement DH by using the following parameters:

- $g = 5$ and
- $p = 37$.

To generate Alice's and Bob's public keys (A and B) you will need to generate random numbers (one for Alice and one for Bob). Finally, to turn the common computed value into a key, you need to hash it and create a 128 bits of key material. Produce screenshots to show your program in action. Encrypt a dummy message of your choice and show the decryption as well. Finally, answer the following questions;

1. The security of a D-H key exchange protocol is based on?
2. The D-H key exchange protocol is vulnerable to?
3. What is the condition for selecting a good value of p in a D-H key exchange protocol?