Cybersecurity

Professor: F. d'Amore

A.Y. 2022/23

Table of Contents

List of Figures

List of Tables

1 Introduction

2 Symmetric Encryption

Secret key cryptography involves the use of a single key. Given a message (the plaintext) and the key, encryption produces unintelligible data which is about the same length as the plaintext was.
Secret key cryptography is sometimes referred to as **conventional cryptography** or **symmetric cryptography**.
Secret key encryption schemes require that both the party that does the encryption and the party that does the decryption share a secret key. We will discuss two types of secret key encryption schemes:

- **Stream Ciphers**: This uses the key as a seed for a pseudorandom number generator, produces a stream of pseudorandom bits, and $\oplus$ s (bitwise exclusive ors) that stream with the data. Since $\oplus$ is its own inverse, the same computation performs both encryption and decryption.
- **Block Ciphers**: This takes as input a secret key and a plaintext block of fixed size (older ciphers used 64-bit blocks, modern ciphers use 128-bit blocks). It produces a ciphertext block the same size as the plaintext block. To encrypt messages larger than the blocksize, the block cipher is used iteratively with algorithms called *modes of operation*. A block cipher also has a decryption operation that does the reverse computation.

2.1 Stream Ciphers

Idea: try to simulate one-time pad

1. Define a secret key (seed)
2. Using the seed, generate a byte stream (A.K.A. **Keystream**): i-th byte is a function of:
   (a) only the key (*synchronous* stream cipher)
   (b) both the key and first i-1 bytes of cipher text (*asynchronous* stream cipher)
3. Obtain the ciphertext by bitwise XORing plaintext and keystream

2.2 Stream Ciphers in practice

2.2.1 A5/1

2.2.2 RC-4

2.3 Block Ciphers

3 Data Integrity

4 Public Key Cryptography

5 Digital Signatures

6 Cryptographically Secure Pseudo-Random Number Generators

7 Authentication

8 Secret Sharing

9 Access Control

10 Secure Protocols

11 Firewalls

12 Email Security

13 Web Technologies

14 Web Security

15 Web Tracking