Computer and network security

Beau De Clercq

2020-2021

Contents

1 Introduction

2 Symmetric ciphers

3 Message authentication

3.1 Hash functions

A hash function H is a function that takes input data blocks of length M and returns a hash value of fixed size R.
A cryptographic hash function that also satisfies following conditions:

- One way property: it should be infeasible to find a data object that maps to a predefined hash value.
- Collision free property: it should be infeasible to find 2 data objects that map to the same hash value.
- Use padding to pad up input to fixed length and add the length l of the block in bits.

By satisfying the first two properties, hash functions can be used to determine if data has been altered.
Hash functions can be used in an number of applications:

- Message authentication: to ensure a message hasn't been altered.
- Digital signatures: ensure the authenticity of messages and identity of the sender.
- One-way password file: store hash value of password in plain text file.
- Intrusion/virus detection: store H(f) for each file to determine if files have been modified.
- Pseudorandom function: use H to generate pseudorandom private key.

3.2 Secure Hash Algorithm (SHA)

3.3 Length extension attack and SHA3

3.4 Message authentication

3.5 Message authentication codes

4 Asymmetric encryption

5 Key distribution