**Chapter 1**

**INTRODUCTION**

In cryptography and computer science, a Merkle tree is a tree in which every leaf node is labeled with the hash of a data block and every non-leaf node is labeled with the cryptographic hash of the labels of its child nodes. Hash trees allow efficient and secure verification of the contents of large data structures. Hash trees are a generalization of hash lists and hash chains.

**1.1 Overview**

Historically, cryptography arose as a means to enable parties to maintain privacy of the information they send to each other, even in the presence of an adversary with access to the communication channel. While providing privacy remains a central goal, the field has expanded to encompass many others, including not just other goals of communication security, such as guaranteeing integrity and authenticity of communications and many more sophisticated and fascinating goals. When you shop on the Internet, for example to buy a book at Amazon, cryptography is used to ensure privacy of your credit card number as it travels from you to the shop's server.

In today’s world, digital signatures are an indispensable element for secured communication applications. They are needed, to ensure the authentication of a communication partner, i.e. in web services like Email or chats. They are also needed, to ensure the authentication of a web server for web services like web-shops or online-banking. But digital signatures are not just used in web services. For example, they can also be used to verify the validity of digital passports or other digital documents.

**1.2 Terminology**

The basics that are of great significance for this technical presentation are discussed in chapter 2. The most important invention in cryptography comes in 1976 with the publication of Diffie and Hellman - “New Directions in Cryptography”. In it they introduce the concept of public - key cryptography, a form of cryptography, which generally allows users to communicate securely without having prior access to a shared secret key. This is done by using a pair of cryptographic keys, designated as public key and private key, which are related mathematically.

Chapter 3 and 4 will consider the main problems of the technical seminar - the Merkle tree traversal problem, algorithms for solving it and their comparison. The Merkle tree traversal is the task of finding efficient algorithms to output the authentication data for successive leaves. Thus, this purpose is different from other, better - known, tree traversal problems found in the literature. As elegant as Merkle trees are, they are used less than one might expect. One reason is that known traversal techniques require large amount of computation, storage or both. This means that only the smallest trees can be practically used. However, with more efficient traversal techniques, Merkle trees may once again become more compelling, especially given the advantage that cryptographic constructions based on Merkle trees do not require any number theoretic assumptions.