Applied Cryptography

View PDF

Instructor(s):

Levente Buttyán
István Lám
István Zsolt Berta

Short Description of the Course:
Today, we live in an information based society: we communicate via networks, we store data in the cloud, we use on-line services, and we even socialize on-line. Trust in all these infrastructure and services is indispensable, and information security technologies play a key role in establishing trust in the cyber world. One of the key enablers of information security is cryptography. This course is about the basics of cryptography and its appications for building secure systems. As a matter of fact, cryptography has not always been used properly in practice; indeed, it is very often used in an inappropriate way, which leads to catastrophic failures. Proper application of cryptographic mechanisms is an engineering issue and needs training. This is the key motivation for our course.

This course has two main parts. In the first part, we introduce the basic cryptographic building blocks (such as symmetric and asymmetric key encryption schemes, hash functions, and random number generators) and the basic protocols that use them (such as block encryption modes, MAC functions, and key establishment). In the second part, we show how these building blocks and basic protocols are used in practice to secure network communication protocols, such as TLS and the security protocols in WiFi, and data storage solutions implemented locally in computers and remotely in the cloud. In addition, we explain how cryptography is used for electronic signatures and how the necessary keys are managed by Public Key Infrastructures.

Besides the lectures, during the first part, we require the students to solve homework assignments individually, while during the second part, they have to solve one project assignment in teams.

Aim of the Course:
The objective of the course is to give an introduction to the basics of cryptography, to explain how basic building blocks work, and to demonstrate how secure systems can be engineered by properly using them. Besides the theoretical background, we use lot of illustrative examples and show practical applications. In addition, where appropriate, we give an outlook to the legal and business aspects of using cryptography.

Prerequisites:
Basic knowledge in algebra and probability theory, as well as some familiarity with computer networks and operating systems are welcome, but not strictly required. On the other hand, basic programming knowledge (Python is preferred) is required to accomplish the homework and project assignments.

Detailed Program and Class Schedule:
Part 1: Cryptographic building blocks

- Symmetric key cryptographic primitives
- Block encryption modes and MAC function constructions
- Asymmetric key cryptographic primitives
- Random number generation
- Cryptographic libraries
- Key exchange protocols

Part 2: Applications of cryptography

- Secure communications with the Transport Layer Security (TLS) protocol
- WiFi security protocols (WEP, WPA, WPA2)
- Disk encryption (aka at-rest-encryption)
- Cloud based secure data storage (Tresorit insights)
- DRM and cryptographic file sharing in the cloud (Tresorit insights)
- Public Key Infrastructures
- Electronic signature applications

Methods of Instruction:
The course comprises a series of lectures. In addition, the students receive regular homework assignments in the first part of the course, and a project assignment in the second part of the course. The project contains a design and an implementation phase, and it should be carried out in teams.

Example for homework assignment:
Implement a command line tool for encrypting and decrypting files with AES-CBC
Using the PyCryptodome Python cryptographic library, implement a simple command line tool in Python that encrypts and decrypts files with AES in CBC mode. The tool should get as input the following: operation (encrypt or decrypt), a key string (16 character long), the name of the input file, the name of the output file. The tool should output a randomly generated IV and the encrypted payload in the output file. Use TLS style padding.

Example for project assignment:
Secure file transfer protocol
This programming project is accomplished in groups of 2-3 students. The group has to develop a simplified secure file transfer application that allows a client program to upload, download, and manage files on a remote server. The communication between the client and the server should be encrypted and integrity protected. The user client should also authenticate to the server before file operations are permitted. In the design phase, the protocols should be specified in details. In the implementation phase, the protocols should be implemented using a real cryptographic programming library. Functioning of the file transfer application is also demonstrated by each team in the class.

Textbooks:
N. Ferguson, B. Schneier, and T. Kohno, Cryptography Engineering, Wiley, 2010.
Other on-line resources (papers, web sites) given by the instructors during the course.

Grading:
There is a midterm and a final written test (quiz type). In addition, the performance in the homework and project assignments is also taken into account when determining the final grade, which is calculated as a weighted sum of the results of the two tests, the homework results and the project result (midterm test 25%, final test 25%, homework assignments 25%, project work 25%).

Instructors' bio:

Levente Buttyán received the Ph.D. degree from the Swiss Federal Institute of Technology - Lausanne (EPFL) in 2002. In 2003, he joined the Department of Networked Systems and Services at BME, where he currently holds a position as an Associate Professor and leads the Laboratory of Cryptography and Systems Security (CrySyS Lab). He has done research on the design and analysis of secure protocols and privacy enhancing mechanisms for wired and wireless networks. Recently, he has been involved in the analysis of some high profile targeted malware, such as Duqu, Flame, MiniDuke, and TeamSpy. He published 100+ refereed journal articles and conference/workshop papers. He also co-authored a book on Security and Cooperation in Wireless Networks published by the Cambridge University Press in 2008. Besides research, he has been teaching courses on network security and electronic commerce in the MSc program at BME, and gave invited lectures at various places. He held visiting professor positions at EPFL and at the University of Washington, Seattle. He is also providing consulting services, he has co-founded three IT security companies Tresorit, Ukatemi Technologies, and Avatao.

István Lám is the CEO and co-inventor of Tresorit’s encryption technology. From a very young age, István had a deep interest in security and cryptography. During his time as a University student, István needed a secure cloud service where he could store his personal files and intellectual property securely. Feeling that no option on the market provided the top-tier security he required, István went on to develop and found Tresorit in 2011, deploying the strictest data security measures in the public cloud, backed by the company’s patent-pending cryptographic encryption technology. Prior to founding Tresorit, István worked as a student researcher at the CrySyS Lab and at the Ecole Polytechnique Federale de Lausanne in Switzerland, and he was a student lecturer at the Budapest University of Technology and Economics. Previously, he was a financial advisor at Future Invest and Business Kft in Hungary. In addition, István has spearheaded Challenge24, a 24-hour long programming contest held annually in Budapest. István is a graduate from the Budapest University of Technology and Economics, where he received his B.Sc. and M.Sc. in Computer Engineering (both with highest honors) with a specialty in cryptography engineering.

István Zsolt Berta obtained his PhD and MSc at the CrySyS Lab of the Budapest University of Technology and Economics (BME), he has MBA from Buckinghamshire Chilterns University College, and obtained professional certifications CISA, CISSP and CCSK. István is Head of Information Security Solution Certification at Citi, his team performing the infosec review of new technologies before they can be introduced into the bank's global infrastructure. Previously (from 2013 to 2014), he was information security officer for Citi technology infrastructure in Europe, Middle East and Africa. Before joining Citi (from 2004 to 2012), he was Head of Information Security and head of R&D at Microsec Ltd., a Hungarian Certificate Authority, he also participated in writing EU standards for electronic signatures and public key infrastructure, and also wrote a book on these disciplines.