Course title:
Applied Cryptography

Instructors:
Levente Buttyán, István Lám, István Zsolt Berta

Duration:
Weeks 1-14, 2x2 hours, 4 credits

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 four 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 discuss the concept and the practice of public key infrastructures (PKI) and electronic signatures, including issues such as issuing, using, and revoking public key certificates, the pitfalls of verifying electronic signatures, experiences in building and operating a certification authority (CA), as well as electronic signature laws and regulations in different countries and business models for PKI. In the third part, we deal with the application of cryptographic primitives for engineering secure communication protocols. We discuss in details well-known examples, such as TLS/SSL and the security protocols used in WiFi and other wireless environments. Finally, in the fourth part, we show applications of cryptography for securing cloud services, focusing on secure cloud based data storage, and sharing first hand experience in desiging and building Tresorit, an encrypted storage service in the cloud.

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, besides the technical details, we give an outlook to the legal and business aspects of using cryptography.

Prerequisites:
No special prerequisites are needed; however, basic knowledge in algebra and probability theory, as well as some familiarity with computer networks and operating systems would be an advantage.

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
- Key exchange protocols
- Cryptographic libraries

Part 2: PKI and electronic signature
- Introduction to the Public Key Infrastructure
- Digital signature and electronic signature
- Verification of electronic signature
- Security of Certification Authorities
- Business models and applications

Part 3: Cryptographic protocols for secure communications
- Secure communication protocols (SSL/TLS)
- Wireless security protocols (WiFi security)
- Secure protocols in resource constrained environments (sensor networks, RFID systems)
- Protocols for anonymous communication

Part 4: Application of cryptography in cloud services
- 2-factor authentications, one-time passwords
- Password management and key derivation
- Practical authentication and authorization protocols (Kerberos, SAML and Oauth)
- Disk encryption aka. at-rest-encryption
- Secure mailing – PGP and SMIME (exercise)
- Client side file encryption (Tresorit insights)
- DRM and cryptographic file sharing in the cloud (Tresorit insights)

Methods of Instruction:
The course comprises a series of lectures with classroom exercises. In addition, the students receive reading assignments and 2 homework projects, which they have to solve in teams. There is a midterm test and, at the end of the course, the students have to pass an exam.

Examples for homework project assignment:

Analysis of key exchange protocols:
A description of a session key establishment protocol is given to the student, whose task is to analyze the protocol, to find as many attacks against it as he/she can, and then to fix the protocol such that attacks are eliminated. Typically the protocol to be analyzed can be attacked in more than one ways. Identifying weaknesses without finding a specific attack is also considered as a valuable contribution. When fixing the protocol, the student should apply the protocol design principles that we discuss in class. Even if the student does not find all possible attacks, applying the principles correctly should eliminate both the discovered and the undiscovered attacks. To help the student, some papers are recommended as a reading assignment.

Design of a cloud based cryptographic storage system:
This programming project is accomplished in groups of 3-4 students. The group has to develop a simplified cloud storage system where data is stored in encrypted form and encryption is performed at the client side. The students have to apply what they learned in class to design their cryptographic protocols, and to implement them using a real cryptographic library. They have to develop a client application with a graphical user interface that integrates all their protocol implementations. The server part is also a real (typically Microsoft Azure) cloud service, and the students have to use the API of that service to upload and download files to and from the cloud.

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:
Final grading: 40% project work + 20% midterm + 40% exam

Instructors' Bios:
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. His current research interest is in security of cyber-phisical systems. 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 IT Security in the BSc program at BME, as well as on Computer Security, and Cryptographic Protocols in the MSc program at BME. He held visiting

professor positions at EPFL and at the University of Washington, Seattle. He is also providing consulting services, and he has co-founded four companies Tresorit, Ukatemi Technologies, IT-SEC Expert, and Avatao.

István Lám is the CEO and co-inventor of Tresorit's encryption technology. From a very young age, Istvan had a deep interest in security and cryptography. During his time as a University student, Istvan 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, Istvan 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, Istvan 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, Istvan has spearheaded Challenge24, a 24-hour long programming contest held annually in Budapest. Istvan 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 crytography engineering.

István Zsolt Berta is Business Information Security Officer (Vice President) at Citibank since 2013. He is responsible for Citi Technology Infrastructure teams of Europe, Middle East and Africa countries complying with Citi's information security standards. From 2004 to 2012 he worked for Microsec, a Hungarian certificate authority and PKI service provider, where he was Head of R&D and Operations. István designed the first 'qualified' long-term preservation service provider operating according to the Hungarian e-signature act. He represented the company at international forums including the European Telecommunication Standards Institute (ETSI). He was part of the ETSI specialist task force that wrote European standards on the information security management of preservation service providers. He wrote a book on PKI and electronic signatures, and runs a blog on information security, focusing on cryptography and PKI. István received PhD from the Budapest University of Technology and Economics (CrySyS Lab) in 2006. He earned MBA (2004) from Buckinghamshire Chilterns University College and he also gained industry certifications Certified Information Systems Auditor (2006) and Certified Information Systems Security Professional (2013).