University of Prishtina
Faculty of Electrical and Computer Engineering

Data Security

Lecturer:

Prof. Dr. techn.Blerim Rexha,
blerim.rexha@uni-pr.edu

Description and the aim of course:

Introduction to encryption algorithms, smartcards and their use in real life applications. After finishing this course students should:

- have basic knowledge about cryptography,
- have basic knowledge about symmetric and asymmetric encryption,
- be able to apply different cryptographic algorithms,
- have basic knowledge about smartcards and their usage in real life applications,
- be able to manage public keys, and
- be able to analyze application that use cryptographic algorithms

Volume and ECTS credits:

The course will once e week, it consists of 2h lecturers and 2h exercises per day, i.e. totally 20h. Number credits according to ECTS 6.0.

Mandatory requirements:

None

Desired requirements:

Basic knowledge in one of the following programming languages: C, C++, C#, Java, or Visual Basic.

Course content:

1. **Cryptography**: Introduction in cryptography, Terminology, Steganagrafy, Algorithms.
2. **DES (Symmetric encryption):** Introduction, DES description, DES security, DES variants.
3. **RSA (Asymmetric encryption and algorithms with public keys):** RSA
4. **Hash functions and digital signatures**: One way function, Hash one way functions, MD5, SHA-1, Digital signatures, Encrypting and digital signatures
5. **Managing of private, secret and public keys (PKI) and X.509 certificates:** Key generation, Key exchange, Digital certificates, X.509 certificates, Key verification, Key update, Storing keys, Backup keys, PKI.
6. **PKCS standards (PKCS#1 – PKCS 15):** Description and usage of each standard in practice.
7. **Smartcards I**: Introduction, Smartcard types, Physical and electrical properties, Smartcard operating systems.
8. **Smartcards II:** Data exchange with smartcards (APDU), Smartcard commands.
9. **Smartcards III:**, PC/SC Architecture, Contactless smartcards, Memory structure, Standards, Applications with Contactless smartcards.
10. **Analyzing usage of cryptography in practical cases**: Email encryption, Electronic payments over Internet - E-commerce., Electronic money, Payment systems with smartcards, E-government.

Exercises:

1. Writing an application that uses a DES, dDES and RSA algorithm using a C# as programming language (other languages are optional).
2. Configuring a Certification Authority (CA) and obtaining X.509 certificates from it. Writing an application that manipulates with X.509 certificates using C# as programming language (other languages are optional).
3. Writing an application that reads some data (for example serial number) from EF of smartcard using C++ with MFC as programming language (other languages are optional).
4. Writing an application that reads phone numbers from a SIM card using C++ with MFC as programming language (other languages are optional).
5. Configuring web server to use X.509 certificates (IIS, Apache, and Tomcat) and reading X.509 certificate properties from a web (ASP or JSP) page.

Independent work:

1. Encrypt a text file using X.509 certificate. The encrypted text file should be save in PKCS#7 format.
2. Read and save all phone numbers from SIM card to a text file.
3. Write a command line (DOS-box) program in C, C++, C#, or Java language that shows all certificate properties.

Literature:

Author	***Title***
Bruce Schneier	Applied Cryptography, ISBN=0-471-12845-7, 1996
Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone	Handbook of Applied Cryptography , ISBN: 0-8493-8523-7 1996, available online at: http://www.cacr.math.uwaterloo.ca/hac/
Cryptograpfy Decrypted	H.X. Mel & Doris Baker, ISBN=0-201-61647-5, 2001
C# Data Security	Matthew MacDonald & Erik Johansson, ISBN=1-86100-801-5, 2003