Title

SECURITY FOR MULTIMEDIA APPLICATIONS

Aim

The aim of this course is to provide basic knowledge on techniques for the security of multimedia systems with particular reference to encryption techniques (symmetric and asymmetric key methods), applications of cryptography to security in multimedia environments (secure connections via the web, protection of multimedia documents, etc.)

Program

1. *Introduction* – Purposes, applications and characteristics of the main security issues of multimedia applications. Basic concepts of computer security: identification, authentication, authorization, availability, confidentiality, integrity, fatherhood. Examples and exercises.

2. *Modern Cryptography* – Introduction to cryptography: cryptanalysis, historical notes. Symmetric encryption. Kerckhoffs's principle. Classification of cryptographic systems. Transposition ciphers. The Spartan's scytale, Encryption rail fence, substitution ciphers, Caesar's cipher, mono-alphabetic substitution ciphers. Cryptanalysis for encryption. Mono-alphabetic encryption Playfair. The Vigenere's cipher. The Enigma machine: rotors, the reflessors, the panel power strips, robustness of Enigma. Exercises and application examples.

3. *Steganography* – Examples of historical and modern use of steganography, Steganography to passive striker, steganography to active attacker, steganography generative vs. injection. Steganography Least Significant Bits (LSB), LSB Steganography with jpeg images. Exercises and application examples.

4. *Watermarking e fingerprint* – Main features, visible and invisible watermarking, software applications for watermarking. Fingerprinting applications. Exercises and application examples.

5. *Contemporary encryption* – Cipher One-Time Pad (OTP), Security OTP (demonstration intuitive), security OTP (formal proof), OTP binary reuse of keys with OTP binary, malleability OTP, OTP and stream ciphers. Pseudorandom number generators. Linear congruence algorithm. Block ciphers, the concepts of confusion and diffusion. Avalanche's Criterion. Substitution-permutation networks (SPN). Feistel networks. Demonstration of the algorithm decryption of a Feistel network. Feistel ciphers based on the template. Data Encryption Standard (DES). Other algorithms based on Feistel networks: 3DES. Meet-in-the-middle attack. Blowfish cipher, RC5 cipher, cipher TEA, AES Algorithm. The four transformations AES algorithm. ECB algorithm - Electronic Codebook. CBC algorithm - Cipher Block Chaining, CTR algorithm. Cryptanalysis contemporary. Exercises and application examples.

6. *Biometric security systems* – Introduction, face detection and recognition, fingerprints and iris detection of the main features. Liveness in biometric systems. Exercises and application examples.

Laboratory activity

During the course there are specific laboratory exercises concerning the security of multimedia applications:

(1) Introduction to programming languages for the Web, hypertext markup languages, Scripting languages, languages for CGI scripts, languages for database, Java and HTML5. Examples and exercises. (2) PHP language (part I): Script PHP development environment XAMPP, The configuration file php.ini, Comments and variables in php Arrays in PHP, Operators and Control Structures in PHP, functions, classes and objects. Examples and exercises. (3) PHP language (part II): The special variables, HTTP methods GET and POST, Cookie, create cookies and parameters closely, Inserting a cookie, placing a cookie durable, Cookie multiple, multiple array of cookies, for example cookies for tracking user's choices. Cookies and security, sessions: create a session, functions getlogged.php, mysessionpage.php, mysessionlogout.php. Examples and exercises. (4) MySQL language: Creating a database, some script in php to interface with the database, storing an encrypted password, rules to encrypt passwords, general rules for writing secure web applications. Examples and exercises. (5) Development of a multimedia application form.

FINAL EXAMS

The exam consists of a written test and an oral exam as well as an application project assigned by the teacher. The written test requires you to perform exercises on the matters of course. The oral exam in-depth discussion of some of the topics covered in class.

REFERENCES

[1] William Stallings, *Cryptography and Network Security - principles and practice*, Prentice Hall, 2011.
[2] B. Forouzan "*Cryptography and Network Security*" Prima edizione, McGraw Hill, 2009.
[3] A.S. Tanembaum, D.J. Wetherall, *Reti di Calcolatori,* (Quinta Edizione), Pearson, 2011.
[4] Teaching material and slide provided by the teacher.