Titolo del Corso
SICUREZZA PER LE APPLICAZIONI MULTIMEDIALI

Nome del Docente
Prof. Gian Luca Foresti

Indirizzo e-mail
gianluca.foresti@uniud.it

Indirizzo Pagina Web Personale
http://users.dimi.uniud.it/~gianluca.foresti/index.html

Crediti (CFU)
6 CFU

Finalità e obiettivi formativi
La finalità principale del Corso è quello di fornire le conoscenze di base sui metodi e sulle tecniche per la sicurezza delle reti e dei sistemi multimediali con particolare riferimento a tecniche di crittografia (metodi a chiave simmetrica e asimmetrica), ad applicazioni della crittografia alla sicurezza in ambito multimediale (connessioni sicure via web, protezione di documenti multimediali, etc.)

Prerequisiti
Sono prerequisiti del corso la conoscenza della matematica di base (in particolare, logaritmi, esponenziali, derivate, integrali, successioni aritmetiche e geometriche, funzioni, aritmetica modulare), dei sistemi operativi e delle reti di calcolatori (architettura di rete, protocolli, sistemi client/server, etc.)

Conoscenze e abilità da acquisire
Lo/la studente/essa dovrà conoscere i concetti fondamentali delle tecniche e degli algoritmi per la sicurezza delle trasmissioni dei dati multimediali (immagini, video, tracce audio, etc.) attraverso la rete internet o più in generale attraverso canali di comunicazione non sicuri. Lo/la studente/essa dovrà inoltre sapere analizzare e comprendere gli elementi basilari delle tecniche di crittografia sia a chiave simmetrica (o privata) che a chiave asimmetrica (o pubblica).
Lo/la studente/essa acquisirà inoltre specifiche capacità trasversali relative all'abilità ad identificare le tecniche e/o i protocolli per la sicurezza più adatti alla trasmissione di dati multimediali sulla rete internet. Specifiche abilità comunicative saranno sviluppate con un'attività mirata alla presentazione di relazioni tecnico-scientifiche e allo sviluppo di applicativi che prevedano la trasmissione sicura di dati multimediali attraverso la rete.

Programma
1. *Introduzione* – Scopi, applicazioni e caratteristiche delle principali problematiche di sicurezza delle applicazioni multimediali. Concetti di base della sicurezza informatica: identificazione, autenticazione, autorizzazione, disponibilità, riservatezza, integrità, paternità. Esercizi ed esempi applicativi.

2. *Crittografia moderna* – Introduzione alla crittografia: crittoanalisi, cenni storici. Crittografia moderna. Modello di cifratura simmetrico. Principio di Kerckhoffs. Classificazione dei sistemi crittografici. Cifrari a trasposizione. La scitale spartana, Crittografia rail fence, Cifrari a sostituzione, Cifrario di Cesare, Cifratura a sostituzione monoalfabetica. Crittanalisi per cifratura. monoalfabetica Cifratura Playfair. Cifrari polialfabetici, Il cifrario di Vigenère. La macchina Enigma.I rotori, il riflessore, il pannello a prese multiple, robustezza di Enigma. Esercizi ed esempi applicativi.

3. *Steganografia* – Esempi storici e moderni di utilizzo della steganografia, Steganografia ad attaccante passivo, Steganografia ad attaccante attivo, Steganografia generativa vs. iniettiva. Steganografia Least Significant Bits (LSB), Steganografia LSB con immagini jpeg. Esercizi ed esempi applicativi.

4. *Watermarking e fingerprint* – Principali caratteristiche, Watermarking visibile, Watermarking invisibile, Software per applicazioni di watermarking. Applicazioni di Fingerprinting. Esercizi ed esempi applicativi.

5. *Crittografia contemporanea* - Cifrario One-Time Pad (OTP), Sicurezza di OTP (dimostrazione intuitiva), sicurezza di OTP (dimostrazione formale), OTP binario, riutilizzo delle chiavi con OTP binario, malleabilità di OTP, OTP e cifrari a flusso. Generatori di numeri pseudocasuali. Algoritmo a congruenza lineare. Cifrari a blocco, i concetti di

confusione e diffusione. Criterio di Avalanche. Reti a sostituzione-permutazione (Substitution-Permutation Networks, SPN). Le reti di Feistel. Dimostrazione dell'algoritmo di decifratura di una rete di Feistel. Cifrari basati sul modello di Feistel. Algoritmo DES – Data Encryption Standard. Altri algoritmi basati su reti di Feistel: 3DES. Meet-in-the-middle attack. Cifrario Blowfish, Cifrario RC5, Cifrario TEA, Algoritmo AES. Le 4 trasformazioni dell'algoritmo AES. Algoritmo ECB – Electronic Codebook. Algoritmo CBC – Cipher Block Chaining, Algoritmo CTR – Counter. Crittanalisi contemporanea. Esercizi ed esempi applicativi.

6. *Sistemi di sicurezza biometrici* – Introduzione, face detection e recognition, impronte digitali e rilevamento delle caratteristiche principali dell'iris. Liveness nei sistemi biometrici. Esercizi ed esempi applicativi.

Attività di Laboratorio

Durante il corso sono previste specifiche esercitazioni di laboratorio relative alla sicurezza delle reti e delle applicazioni multimediali:
(1) Introduzione ai linguaggi di programmazione per il WEB, Linguaggi di marcatura ipertestuale,
Linguaggi di scripting, Linguaggi per script CGI, Linguaggi per database, Java e HTML5, Esempi ed esercizi
(2) Linguaggio PHP (parte I): Script PHP, Ambiente di sviluppo XAMPP, Il file di configurazione php.ini, Commenti e variabili in php, Array in PHP, Operatori e Strutture di controllo in PHP, Funzioni, classi e oggetti, Esempi ed esercizi.
(3) Linguaggio PHP (parte II): Le variabili speciali, metodi HTTP GET and POST, i Cookie, creare I cookie e i parametri da vicino, Inserimento di un cookie, inserimento di un cookie durevole nel tempo, Cookie multipli, Array di cookie multipli, esempio di cookie per il tracciamento delle scelte dell'utente. I Cookie e la sicurezza, Le sessioni: creare una sessione, funzioni getlogged.php, mysessionpage.php, mysessionlogout.php. Esempi ed esercizi.
(4) Linguaggio MySQL: Creazione di un database, alcuni script in php per l'interfacciamento con il database, memorizzazione di una password cifrata, regole per cifrare le password, regole generali per scrivere applicazioni web sicure. Esempi ed esercizi.
(5) Sviluppo di un'applicazione multimediale sicura.

Bibliografia

[1] William Stallings, *Cryptography and Network Security - principles and practice*, Quinta edizione, Prentice Hall, 2011 (ISBN-13: 978-0-13-705632-3).
[2] B. Forouzan "*Cryptography and Network Security*" Prima edizione, Mc Graw Hill, 2009.
[3] A.S. Tanembaum, D.J. Wetherall, *Reti di Calcolatori,* (Quinta Edizione), Pearson, 2011.

Il materiale didattico, le slide e le riprese video delle lezioni del docente saranno resi disponibili sulla piattaforma di e-learning dell'Ateneo di Udine. Tali materiali sono riservati ai soli studenti iscritti al Corso.

Modalità d'esame

L'esame si compone di una prova scritta e di una prova orale oltre che dello svolgimento di un progetto applicativo assegnato dal docente. La prova scritta richiede di svolgere esercizi inerenti gli argomenti del Corso. La prova orale consiste nella discussione approfondita di alcuni degli argomenti trattati a lezione.

Orario di ricevimento

L'orario di ricevimento è concordato all'inizio del corso con gli studenti e pubblicizzato attraverso Esse3. Gli studenti possono chiedere per e-mail ricevimenti aggiuntivi oltre a quello standard.