Teoria dell'informazione e codici
per Ingegneria Elettronica – 6 crediti

1. DESCRITTORI

1.1 SSD: ING-INF/03
1.2 Crediti: 6
1.3 Docente: Roberto Cusani
1.4 Calendarizzazione: primo semestre
1.5 Offerto a: SELR2
1.6 Tipologia di valutazione: esame SCRITTO E ORALE con votazione in trentesimi

2. OBIETTIVI DEL MODULO E CAPACITÀ ACQUISITE DALLO STUDENTE

ITA

Conoscenza dei principi della teoria dell'informazione quali la quantità di informazione, la codificazione di sorgente e di canale. Principali codificatori di sorgente usati nelle applicazioni. Conoscenza dei codici a blocchi e dei codici convoluzionali, delle principali tecniche usate nella pratica e delle loro prestazioni. Strategie di co-decodificazione.

Conoscenze di base sulla crittografia simmetrica e asimmetrica e dell'hashing. Tecniche di cifratura più comuni e loro applicazione.

Introduzione ai Sistemi biometrici, alla Steganografia e al watermarking

ENG

This course will set out the fundamental concepts of information theory as well as source and channel coding. The topics covered in the class range from the mostly used source encoders to a deep description and performance analysis of principal channel coding techniques such as block codes, convolutional codes, turbo codes.

Besides a brief introduction on cryptography (symmetric and asymmetric ciphers) and hashing techniques is given.

The last part of the course covers topics about biometric systems and steganography/watermarking.

3. PREREQUISITI

ITA

Conoscenza dei principi del calcolo delle probabilità, della statistica, delle trasmissioni numeriche.

ENG

Basic concepts about probability, statistics, digital transmission

4. RISULTATI DI APPRENDIMENTO ATTESI

ITALIANO

Conoscenza delle proprietà di compressione dei codici di sorgente, e dei rispettivi campi di applicazione. Capacità di distinguere le diverse tipologie di codificazione di canale in base alle differenti capacità di rivelazione e/o correzione di errore, e gli ambienti applicativi per i quali risultano più adeguate.
Distinzione tra crittografia simmetrica e asimmetrica, e hashing, e dei differenti campi di applicazione.
Conoscenza dei fondamenti della biometria.

INGLESE

Knowledge of source encoders, their compression efficiency, and their applications. Deep comprehension of error detection and error correction capabilities of a channel code as well as the principles on which the dimensioning of a protection strategy relies on. Understanding of the differences between symmetric and asymmetric ciphering and between ciphering and hashing, and the different application fields.
Knowledge of the fundamentals of biometrics.

5. PROGRAMMA

ITA

0. L'informazione, il canale trasmissivo e la sua codifica
1. Codifica di sorgenti discrete, Entropia di sorgente, codice di Huffman, primo teorema di Shannon: Algoritmi di compressione per dati, voce ed immagini
2. Codici per la rivelazione e la correzione degli errori (CRC, ARQ e FEC)
3. La trasmissione di codici a blocco su canali binari, Aritmetica modulo 2 e Campi di Galois
4. Codici a blocco lineari, Codici duali e Codici ciclici
5. Codici a blocco di comune impiego, checksum, CRC, Rappresentazione polinomiale e circuitale
6. Codici convoluzionali, decodifica a massima verosimiglianza hard e soft, algoritmo di Viterbi, interallacciamento, codifica concatenata
7. Canali numerici: Modello del collegamento numerico, Entropia di canale, Flusso medio di informazione, Capacità di canale, Disuguaglianza di Fano, Secondo Teorema di Shannon
8. Turbocodici: Codici convoluzionali recursivi sistematici (RSC), Punturazione, Concatenazione in parallelo, Soft – output Viterbi algorithm (SOVA) e decodifica iterativa
9. Crittografia: storia, concetti fondamentali e definizioni, chiave pubblica e privata, algoritmi DES, cenni su AES, RSA; Hash e Hash sicuro (SHA); firma digitale
10. Sistemi biometrici, Cenni su steganografia e su watermarking

ENG

0. Information, transmission channel and coding principles;
1. Discrete source coding. Entropy, Huffman code, First Shannon Theorem; Data, voice and images compression algorithms;
2. Codes for error detection and correction (CRC, ARQ e FEC);
3. Block codes transmission over binary channels, Galois fields and module-2 arithmetics;
4. Linear block codes, dual codes and cyclic codes;
5. Common block codes, checksum, CRC, polynomial representation, circuital implementation
6. Convolutional codes: Maximum likelihood hard and soft decoding, Viterbi algorithm, interleaving, concatenated codes;
7. Discrete channels: digital channel modeling, channel entropy, information rate, channel capacity, Fano's inequality, Second Shannon's theorem on channel coding;
8. Turbo codes: Recursive sistematic convolutional codes (RSC), puncturing, parallel concatenation, soft output Viterbi algorithm (SOVA), iterative decoding;
9. Cryptography: history, fundamentals and definition, private and public key, algorithms: DES, AES, RSA; Hash and SHA; digital signature;
10. Biometric systems, Principles of steganography and watermarking

6. MATERIALE DIDATTICO

Per le sezioni da 1 a 8:

- Teoria dell'Informazione e Codici, R. Cusani-T. Inzerilli, ed. Ingegneria 2000, Settembre 2008
- Esercizi di Teoria dell'Informazione e Codici, R. Cusani-T. Inzerilli, ed. Ingegneria 2000, Dicembre 2006
- Materiale integrativo distribuito dal docente

Per le sezioni da 9 a 10:

- Lucidi del corso, distribuiti dal docente.
- Materiale integrative distribuito dal docente

7. SITO WEB DI RIFERIMENTO

http://infocom.uniroma1.it/~robby/tic1/cusani_prog_tic.html
http://infocom.uniroma1.it/~robby/

Curriculum del docente prof. Roberto Cusani:

http://infocom.uniroma1.it/~robby/cusani_CV_italiano.htm
http://infocom.uniroma1.it/~robby/cusani_CV_English.html