Università degli Studi di Trieste

Dipartimento di
Matematica e Geoscienze

prof. Francesco Fabris
Dipartimento di Matematica e Geoscienze
via Valerio 12/b
34127 TRIESTE
+39 040 558 2625
ffabris@units.it

217MI – **Complexity and Cryptography** - 9 cfu - 72 h - I year - II Semester

Introduction to Automata Theory

finite automata; nondeterminism; regular expressions; non regular languages; context-free grammars; pushdown automata.

Computability theory

Algorithm as effective procedure; Unlimited Register Machine (URM); URM-computable functions; generation of computable functions by concatenation, substitution, recursion, limited and unlimited minimalization; Ackermann's function.

Gödel arithmetization, programs Gödelization, numbering of computable functions; Cantor diagonalization, existence of non computable functions, examples of non-computable functions; the s-m-n theorem, universal programs.

Decidability and undecidability; undecidability and the halting problem, undecidability of 'Phi_x is total', 'Phi_x = 0', 'Phi_x = Phi_y', Rice's theorem, recursion and fixed point theorem.

Other approaches to computability; notes on Gödel-Kleene model of partial recursive functions and recursive primitive functions; the Turing Machine (TM), equivalences between different TM models, contraction and extension of a TM, examples.

Equivalence between different computational models and Church-Turing thesis. Background on recursive sets and recursively enumerable sets.

Computational complexity

Polynomial algorithms and intractable problems, P and NP complexity classes, relation between P and NP class; reductions in polynomial time, the class of NP-complete problems, Cook theorem (notes), examples of NP-complete problems, the structure of the NP class.

Cryptography

The Shannon cryptographic communication system; problems related to data security: interception, impersonation, data integrity violation.

Mathematical Preliminaries:

Background on probability distribution and convexity of functions, Jensen's inequality, log-sum; introduction to Mutual Information and Entropy; background on number theory and on some arithmetic and modular functions.

Secret key encryption:

Substitution and transposition ciphers; nomenclators, homophonic ciphers, statistical cryptanalytic attacks, polyalphabetic and Vigenère cipher, the principle of confusion and diffusion, rotor machines, the problem of key exchange in a network of N users.

Shannon approach; pure ciphers, residual classes of messages and cryptograms, equivocations, fundamental inequality of encryption, ideal and perfect ciphers, ideality of transposition cipher, the perfected state, cipher weakening as a function of the cryptogram length, one-time pad cipher and its perfection, unicity distance and its calculation for different ciphers.

Block ciphers; DES (Data Encryption Standard), S-box and Feistel function, brief notes on IDEA and AES.

Symmetric and asymmetric encryption, Shamir's protocol, general principles of the digital signature.

Stream ciphers; random generators and random characters, pseudo-random generators and Golomb criteria, linear feedback shift registers as generators, linear complexity and known-plaintext attack, nonlinear registers.

Public key encryption:

one-way functions, the finite logarithm and the key exchange, partial sums and the knapsack cipher, RSA cipher.

Digital signature, data integrity and extracts, DES used as a hash function.

Outline on protocols.

Prof. Francesco Fabris