Protocols, cryptanalysis and mathematical cryptology

Lecturers
Olivier MARKOWITCH (Coordinator), Liran LERMAN and Christophe PETIT

Course mnemonic
INFO-F514

ECTS credits
5 credits

Language(s) of instruction
English

Course period
Second term

Course content

Secret Sharing. Oblivious transfer. Fair exchange protocols. Electronic commerce. Digital signatures.

Differential and linear cryptanalysis.

Elliptic curve cryptography.

Cryptographically strong random generators. Serial encryption.

Arithmetic algorithms and representation of large numbers. Factoring, primality testing, discrete logarithm, prime numbers generation... Original methods: biometrics, visual cryptography, quantum cryptography...

Objectives (and/or specific learning outcomes)

Research methods in cryptology.

Modern cryptology and cryptanalysis tools; design and analysis of cryptographic primitives and protocols.

Critical analyzis of some current issues in the field.

Pre-requisits and co-requisits

Course having this one as co-requisit

INFO-Y099 | Multicore programming | 6 crédits

Teaching method and learning activities

Short theoretical introduction, interactive presentation and analysis of research papers, general discussion.

Contribution to the teaching profile

Acquire deep knowledge in cryptology, assimilate new concepts, develop a rigorous approach of scientific reasoning, develop abstraction with the aim of an analysis and of a scientific approach, present orally or in writing in a clear, concise and rigorous way the results of a work, develop a scientific argumentation, summarize and synthesize.

References, bibliography and recommended reading

Darrel Hankerson, Alfred J. Menezes et Scott Vanstone, "Guide to Elliptic Curve Cryptography", Springer, 2003.

Henk C. A. van Tiborg ed., "Encyclopedia of Cryptography and Security", Sringer, 2005.

Mitsuru Matsui, "Linear cryptanalysis method for DES cipher" in Advances in Cryptology, EUROCRYPT'93, LNCS #765,Springer-Verlag, pp.386-397, 1994.

Eli Biham et Adi Shamir, "Differential Cryptanalysis of the Data Encryption Standard", Springer Verlag, 1993.

Other information

Contact(s)

Yves Roggeman - Computer Science Dept - Campus Plaine - CP212 - Building N/O, Room 2.N8.115 Email: yves.roggeman@ulb.ac.be

Olivier Markowitch - Computer Science Dept - Campus Plaine - CP212 - Building N/O, Room 2.N8.115A Email: olivier.markowitch@ulb.ac.be

Evaluation method(s)

Other

Evaluation method(s) (additional information)

Preparation and presentation of seminar subject

Determination of the mark (including the weighting of partial marks)

Seminar presentation and active participation during the course

Main language(s) of evaluation

English and French

Programmes

Programmes proposing this course at the faculty of Sciences

MA-INFO | Master in Computer science | finalité Professional/unit 1 and finalité Professional/unit 2 and MA-SECU | Master in cybersecurity | finalité Cryptalalysis and Forensics/unit 1 and finalité Corporate Strategies/unit 1