Cryptography

Lecturer :Tovondrainy Christalin Razafindramahatsiaro talin@aims.ac.za, christalin@univ-antananarivo.mg
(University of Antananarivo)

Introductory course. This course is an introduction to cryptographic issues cryptographic problems, and the mechanisms that guarantee the security of an information information exchange. We deal with the most classical cryptosystems as examples:
- Cryptosystems, cryptographic attacks
- Perfect security, semantic security
- Symmetric cryptography, block ciphers, stream ciphers
- Asymmetric cryptography: hard problems and trapdoor functions, RSA, El Gamal encryption... review of some attacks.
- Protocols : key exchange, signature, proofs without information.

Post Quantum Cryptography. The goal is to present some cryptosystems that already exist and and intended even after the realization of quantum computers.
- Problem
- Code-based cryptosystems
- Cryptosystems based on euclidean networks
- Multivariate (public key) cryptography

Another part of the course consists in informing the audience about some rules and and recommendations concerning the cryptographic key management, authentication and threat analysis methods..
- On cryptographic computation records
- Study of the size of the keys
- On the evolution of key sizes
- Security equivalence between symmetric key sizes and asymmetric module.