Public key cryptography: an introduction

Cryptology is defined as the science of storing, managing, transmitting and transforming information in untrusted environments. The area of public key cryptography considers scenarios in which the involved users do not share a priori high entropy secrets, and must moreover communicate using insecure channels.

This course is an introduction to this fascinating area, focusing on the mathematical foundations behind the cryptographic constructions. We will present several cryptographic constructions for different application scenarios (e.g. encryption, signatures, key exchange schemes), and also introduce a few advanced tools (e.g. oblivious transfer, zero knowledge proofs). Further, it is our goal to give students basic techniques for understanding and developing cryptographic proofs and recognizing their practical implications.

Outline of Sessions

1. Introduction to Cryptography (notes provided by M.I. G. Vasco)
2. Key establishment, Encryption Schemes.
    a. KE; motivation, rationale– Example 1.; DH [Lecture notes by Ronald Rivest]
    b. PK Encryption – Examples 1 and 2: El Gamal, RSA [Chapter 8, book by Barakat et al.]
    c. Computational Assumptions [Lecture notes by D. Poincheval]
    d. Provable security basics: security models, security notions for KE and PKE, game-based proofs [Lecture notes by D. Poincheval]
    e. Security proofs: examples [Lecture notes by D. Poincheval]

3. Signature Schemes

    Main source: [Lecture notes by D. Poincheval]

4. Cryptanalysis (practical session!)
5. Advanced Topics (for exciting applications)

a. Multiparty Computation/Secret Sharing Schemes [Pdf by Cohen] [D. Wagner's lecture notes]
b. ZKP [Lecture notes by Boaz Barak]