An introduction to applications of algebra and number theory in the field of cryptography. In particular, the use of elliptic curves in cryptography is studied in great detail.

- Introduction to cryptography and in particular to public key systems, RSA, Diffie-Hellman, ElGamal.
- Finite fields, construction of all finite fields, efficient arithmetic in finite fields.
- Elliptic curves, the group law of an elliptic curve, methods for counting the number of points of an elliptic curves over a finite field: Baby-step giant step, Schoof’s method.
- Construction of elliptic curves based cryptographic systems.
- Methods for prime decomposition, the elliptic curves method, the quadratic sieve method.
- Safety of public key cryptographic methods.