אוניברסיטת
בן-גוריון בנגב

# The Department of Mathematics

2015–16–B term

**Course Name** Arithmetic methods in cryptography

**Course Number** 201.1.3121

**Course web page**
`https://www.math.bgu.ac.il/~bessera/crypto/`

**Lecturer** Prof. Amnon Besser, <bessera@bgu.ac.il>, Office 212

**Office Hours** `https://www.math.bgu.ac.il/en/teaching/hours`

## Abstract

## Requirements and grading[1]

## Course topics

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 filelds, 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.

[1] Information may change during the first two weeks of the term. Please consult the webpage for updates