אוניברסיטת בן-גוריון בנגב
הפקולטה למדעי הטבע – המחלקה למדעי המחשב
סמסטר א' תשע"ג

סילבוס קורס

שם הקורס: **קריפטוגרפיה**
Cryptography

מס' קורס: **202-1-5351**

סוג קורס: קורס בחירה
נק"ז: 4.0

מרצה הקורס: פרופ' עמוס ביימל

דרישות קדם: תכנון אלגוריתמים 202-1-2041; הסתברות 201-1-2391.

This course is intended for third-year undergraduate students as well as for graduate students.

מטרת ונושא הקורס

Modern cryptography provides algorithms and protocols for protecting honest parties from distrusted or malicious parties that can eavesdrop to communication or modify it. Basic topics in cryptography include secure encryption, digital signatures, and authentication.
In this course we will discuss these topics, their realizations, and applications. The material covers cryptosystems that are both practical and theoretically interesting. To achieve this goal, we'll also teach some background in number theory that is necessary to understand modern cryptosystems such as *RSA*.

Topics:

1. Classical encryption systems and perfect encryption systems
2. Symmetric encryption, DES, AES
3. Number theory background
4. Public encryption, RSA, and ElGamal encryption systems
5. Digital signatures
6. Cryptographic hashing and authentication
7. Secret sharing, private information retrieval, and introduction to secure computation

ספרות הקורס

1. D. R. Stinson. *CRYPTOGRAPHY: Theory and Practice.* Third Edition, CRC Press. 2005
2. Jonathan Katz and Yehuda Lindell. *Introduction to Modern Cryptography.* Chapman & Hall/Crc Cryptography and Network Security Series, 2007.