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

סילבוס קורס

שם הקורס: **קריפטוגרפיה**
Cryptography

מס' קורס: **202-2-5871**

סוג קורס: קורס בחירה
נק"ז: 4.0

מרצה הקורס: מר אורי שטמר ופרופ' עמוס ביימל

דרישות קדם: תכנון אלגוריתמים 202-1-2041; הסתברות 201-1-2391 (או קורס מקביל).

מטרת ונושא הקורס

קריפטוגרפיה מודרנית היא ענף במדעי המחשב העוסק בפיתוח שיטות לאבטחת מידע דיגיטלי, למשל, כנגד יריב (צד שלישי) המסוגל להאזין לשיחה בין שני מחשבים. נושאים בסיסיים בקריפטוגרפיה כוללים הצפנה, חתימות דיגיטליות ואימות של הודעות. בקורס נדון בנושאים אלו, במימושם ובאפליקציות שלהם. חומר הקורס כולל הן מערכות קריפטוגרפיות מעשיות והן מערכות קריפטוגרפיות בעלות ערך תיאורטי. בנוסף, חומר הקורס כולל רקע מתמטי מתורת המספרים שדרוש על מנת להציג ולנתח את המערכות הקריפטוגרפיות הנ"ל, כמו למשל RSA.

נושאים:

1. מערכות הצפנה קלאסיות והצפנה מושלמת.
2. הצפנה סימטרית, DES, AES.
3. רקע מתמטי מתורת המספרים.
4. הצפנה במפתח פומבי, RSA, ElGamal.
5. חתימות דיגיטליות.
6. פונקציות hash קריפטוגרפיות, ואימות של הודעות.
7. נושאים מתקדמים כגון: חלוקת סוד, אחזור פרטי של מידע, פרטיות דיפרנציאלית ומבוא לחישוב בטוח.

נושאים נוספים עלולים להיכלל בחומר הקורס בהתאם לשיקול המרצים.

English Syllabus

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. Introduction to 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, differential privacy and introduction to secure computation.

Additional topics may be covered in the course.

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.