קריפטוגרפיה וסיבוכיות - 236508

מרצה: ד"ר ארז פטרנק (חדר 528, טלפון 4942, שעות קבלה: ה' 30 :15-30 :14)

בודק תרגילים: בני אפלבאום (חדר Taub 325 , טלפון 4307)

שעות הרצאה: יום ג' 30 :12-30 :10.

דרישות קדם: תורת החישוביות 236343, וקריפטולוגיה מודרנית 236506.

אתר הקורס: http://www.cs.technion.ac.il/~erez/courses/cc/ .

בעבר הייתה הקריפטוגרפיה אוסף של אלגוריתמים בלתי תלויים המיועדים להצפנת מידע. לחלק מהאלגוריתמים היה בסיס מתמטי מתורת המספרים ולחלק אחר היה בסיס "אינטואיטיבי" שהתבסס על שבירות ידועות מהעבר. ב- 20 השנים האחרונות החלו ניסיונות לפתח בסיס מדעי להצפנות תוך שימוש בכלים מתורת הסיבוכיות. נשאלו שאלות כגון: מהי הצפנה בטוחה? מה ניתן (או לא ניתן) להוכיח על פרוטוקולים קריפטוגרפיים? וכיו"ב. כיום תופסת הקריפטוגרפיה מקום מרכזי במדעי המחשב התיאורטיים. בקורס נציג את מושגי היסוד התיאורטיים של הקריפטוגרפיה.

הנושאים העיקריים שיילמדו בקורס יהיו:

1. פונקציות חד-כיווניות וביטים קשים שלהן.
2. סדרות פסאודו-אקראיות, וייצורן על-סמך תמורות חד-כיווניות.
3. פונקציות הצפנה חזקות בעלות מפתח פומבי.
4. שיטות חתימה בטוחות.
5. הוכחות באפס מידע.
6. חישובים פרטיים מבוזרים.

חומר הלימוד המומלץ הוא:

1. O. Goldreich, “Foundation of Cryptography - Basic Tools”, Cambridge University Press, 2001.
2. O. Goldreich, Foundation of Cryptography - Fragments of a Book (1995), available at: http://www.wisdom.weizmann.ac.il/home/oded/public_html/frag.html .

הציון בקורס יינתן על-סמך פתרון תרגילי בית (כ- 4 עד 5), השתתפות בהרצאות, ואם יהיה צורך – גם בחינה סופית.