נושאים מתקדמים במדעי המחשב:
נושאים נבחרים בקריפטוגרפיה (236613)

מרצה:	פרופ' יובל ישי
בודק תרגילים:	ויקטור קולובוב
שעות הרצאה:	א' 30 :14-30 :12
דרישות קדם:	תורת החישוביות (236343) קריפטולוגיה מודרנית* (236506) *יתאפשר רישום ידני גם ללא דרישת קדם זו.

תאור הקורס

הקורס עוסק בתיאוריה של קריפטוגרפיה ומהווה מבוא למחקר עדכני בתחום. המוטיבציה למרבית הבעיות בהן נעסוק נובעת מהשאלה הכללית הבאה: כיצד ניתן להגן על חישוב המערב מספר משתתפים מפני יריב המנסה ללמוד מידע אסור או לשבש את נכונות החישוב? שאלה זו תטופל במגוון של הקשרים שונים, התלויים בסוג החישוב המבוצע, בכוחו של היריב, במידת ההגנה הנדרשת ובדרישות היעילות.

בין הנושאים שיכוסו:

- סקירה של פרימיטיבים קריפטוגרפיים בסיסיים: פונקציות חד-כיווניות, פסאודו-אקראיות, הצפנה, חתימה דיגיטלית, התחייבות, הוכחות באפס-מידע, חלוקת סוד.
- פרוטוקולים לחישובים בטוחים. לדוגמא: כיצד יכולים שני מיליונרים להחליט מי עשיר יותר מבלי לחשוף כל מידע נוסף על מידת עושרם? כיצד ניתן לשלוף פריט מידע ספציפי מתוך בסיס נתונים מבלי לחשוף דבר על זהות הפריט המבוקש?
- הצפנה הומומורפית: כיצד ניתן לבצע חישובים על מידע מוצפן מבלי לפגוע בסודיות ההצפנה?

הקורס בעל אופי תיאורטי ודורש בגרות מתמטית. הוא מומלץ במיוחד לסטודנטים אשר למדו את הקורס תורת הסיבוכיות (236313) או קורסים מתקדמים אחרים בתיאוריה של מדעי המחשב. עם זאת, קורסים אלו אינם מהווים דרישת קדם, והרקע הנדרש יינתן במהלך הקורס.

דרישות הקורס

הציון הסופי יקבע ע"י 2-3 תרגילי בית (50%), בחינה סופית **קלה** (40%) והשתתפות בכיתה (10%).

תוצרי למידה

בסיום הקורס הסטודנטים: 1) ידעו כיצד להגדיר בטיחות של פרוטוקולים קריפטוגרפיים; 2) יכירו תוצאות בסיסיות של אפשרות ואי-אפשרות של חישובים בטוחים; 3) ידעו כיצד לבנות פרוטוקולים לחישובים בטוחים של פונקציות כלליות.