קריפטוגרפיה וסיבוכיות (236508)
אביב תשפ״ג

מרצה:	פרופ׳ יובל ישי, טאוב 525, yuvali@cs
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. בעבר הייתה הקריפטוגרפיה אוסף של אלגוריתמים בלתי תלויים המיועדים להצפנת מידע, אשר האמונה בבטיחותם נסמכה על עמידה בפני שיטות שבירה ידועות. ב-30 השנים האחרונות פותח בסיס מדעי משותף לשיטות הצפנה שונות תוך שימוש בכלים מתורת הסיבוכיות. בנוסף, תחום העיסוק של הקריפטוגרפיה הורחב לשאלות רבות נוספות העוסקות בשמירה על סודיות ושלמות של מידע. כיום תופסת הקריפטוגרפיה מקום מרכזי במדעי המחשב התיאורטיים. בקורס נציג את מושגי היסוד של תיאוריה זו.

בין הנושאים שיכוסו בקורס:

- הצפנה
- פונקציות חד-כיווניות וביטים קשים שלהן
- פסאודו-אקראיות: בניות ושימושים
- חתימות דיגיטליות
- הוכחות באפס-מידע
- חלוקת סוד וחישובים בטוחים

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 כ-3 תרגילי בית (50%), בחינה סופית **קלה** (40%) והשתתפות בכתה (10%).