



סילבוס מבוא לקריפטוגרפיה
203.3444/203.4444
אביב 2010

מרצה:	ד"ר אור דונקלמן
הרצאה:	יום ג', 16:10-19:00 בניין חינוך, חדר 401
מבחנים:	מועד א' - יום ו', 21.6.11 מועד ב' - יום א', 12.7.11 המבחן הוא בחומר פתוח
ציון:	30% - תרגילי בית מגן (5 תרגילים, כל אחד 6% מגן בנפרד) 70% - מבחן אם ציון המבחן הוא מתחת ל-46, תרגילי הבית לא ילקחו בחשבון
קדם:	שיטות הסתברותיות (203.2480)

נושאי הקורס:

1. מבוא לקריפטוגרפיה
2. צפני החלפה, צופן Vigenere, צופן Vernam (מפתח חד-פעמי)
3. מבוא לתורת האינפורמציה, תורת Shannon למערכות סודיות
4. צפני בלוקים - AES, DES, אופני תפעול, מבוא לקריפטאנליזה
5. פונקציות תמצות קריפטוגרפיות וחתימות חד פעמיות
6. מבוא לתורת המספרים
7. הצפנת מפתח פומבי - אלגוריתם החלפת המפתחות של Diffie-Hellman, אלגוריתם RSA, ווארינטים, מערכות חתימה דיגטלי מבוססות Discrete Logarithm
8. הוכחות באפס ידע - פרוטוקול Fiat-Shamir
9. סכמות לחלוקת סוד

ספרי לימוד:

1. "Cryptography: Theory and Practice", Stinson
2. "Handbook of Applied Cryptography", Menzes, van Oorschot, Vanstone