שם הקורס: נושאים מתקדמים במדעי המחשב

שדות של פונקציות אלגבריות וצפנים של גופא

מספר הקורס 236604

סמסטר חורף תשע"ח

מרצה:	**פרופ' מיכאל קמינסקי**
מתרגל/בודק תרגילים:	
שעות הרצאה:	**א' 10:30 – 12:30**
דרישות קדם:	**אלגברה מודרנית ח' 104134**
אתר הקורס: (כתובת האתר)	

תאור הקורס

הקורס יעסוק בתורה של עקומים אלגבריים (כשני שליש מן הקורס) ושמושם בצפנים האלגבריים-הגיאומטריים של גופא ובסיבוכיות של חישובים אלגבריים מעל שדות סופיים (והשליש הנותר של הקורס). לא נדרש שום רקע בנושאים הנ"ל, אך יש צורך בבגרות מתמטית ובנכונות להשלים השכלה מתמטית תוך השקעה סבירה.

פרשית הלימודים

א) יסודות של תורת השדות של הפונקציות האלגבריות: אתרים, שדות של הפונקציות הרציונליות, אי-תלות של הערכות, מחלקים ודיפרנציאלים, משפט של רימן-רוך ומסקנותיו.

ב) הצפנים האלגבריים-הגיאומטריים של גופא: צפנים, הצפנים של גופא, הצפנים של גופא הקשורים לשדות הפונקציות הרציונליות.

ג) הקשר בין צפנים ואלגוריתמים למכפלת פולינומים מעל שדות סופיים: אלגוריתמים בילינאריים, חסמים תחתונים ועליונים.

דרישות הקורס

בחינה סופית 80%, השתתפות בשיעורים 20%.

רשימת ספרות

H. Stichtenoth, *Algebraic Function Fields and Codes, Springer*, 1993.

D.V. Chudnovsky and G.V. Chudnovsky, Algebraic complexities and algebraic curves over finite fields, *Journal of Complexity* 4 (1988), 285-316.

A. Lempel, G. Seroussi, and S. Winograd, On the Complexity of Multiplication in Finite Fields, *Theoretical Computer Science* 22 (1983), 285-296