

תאריך עדכון: 5.8.2009

תורת המספרים למדעי המחשב 89-256-01

סוג הקורס: שיעור
היקף שעות: 3
סמסטר ב', שנת הלימודים תש"ע

אתר הקורס: www.math.biu.ac.il/~mschein/ntcs.html

תוכן הקורס: תורת המספרים האלמנטרית.
מהלך שיעורים: הרצאה.

נושאי הקורס:

1. מספרים ראשוניים, פירוק לגורמים ראשוניים, שאריות, חפיפה, שדות סופיים.
2. הצפנה ציבורית (RSA) והתקפות עליה, אלגוריתמים לפירוק מספרים לגורמים ראשוניים.
3. הדדיות רבועית, מספרים שלמים של גאוס, שדות רבועיים.
4. שברים משולבים.
5. התפלגות הראשוניים, הפוסטולט של ברטרנד.
6. שיטות הצפנה נוספות.

דרישות קדם: אלגברה לינארית, מתמטיקה בדידה או מבנים אלגבריים. ניסיון עם תוכנות מועיל אך אינו הכרחי.

מרכיבי הציון:

20% תרגילי בית
80% מבחן מסכם

ספרים:

הקורס לא יעקוב אחרי שום ספר. יש הרבה ספרים בתחום שיכולים להועיל לסטודנט, ביניהם:

א' רובינשטיין, תורת המספרים.

H. Davenport, The Higher Arithmetic

G. H. Hardy and E. M. Wright, An Introduction to the Theory of Numbers

נמצא באתר של (W. Stein, An Explicit Approach to Elementary Number Theory) (המחבר)