

נושאים מתקדמים 1 (02360601)

פרופ' רפאל פז	מרצה:
<p>הקורס יועבר במתכונת מיוחדת מול סטודנטים מחו"ל ויפרס על כמה מפגשים בתאריכים מסוימים ולא לאורך כל הסמסטר.</p> <p>פירוט: מסגרת כללית 7.4 עד 6.5</p> <p>7,8 באפריל: שיעור</p> <p>15,16 באפריל: ללא שיעור (חופשת פסח)</p> <p>21, 22 באפריל: שיעור</p> <p>28, 29 באפריל: שיעור (יתכן ויסתיים ב-18.30 בגלל יום הזיכרון)</p> <p>5,6 במאי: שיעור</p>	שעות הרצאה:
-יפורסם בהמשך-	דרישות קדם:
הקורס יינתן באנגלית	הערה:

תיאור הקורס

Course name: Meta-complexity and Cryptography

Description:

Meta-complexity refers to the computational complexity of problems that are themselves about computations and their complexity. Such problems include the Minimum Circuit Size Problem and the Time-bounded Kolmogorov Complexity Problem, the study of which originated in the 1950s/60s and predate the modern study of Complexity theory.

Meta-complexity provides a unifying framework for a variety of central tasks in several areas of computer science, including computational complexity, cryptography, and learning theory, and there has been a recent explosion of works connecting these areas through the lens of Meta-complexity. In this course, we will focus on these recent development, with a particular focus on connections with Cryptography.

Learning outcomes:

By the end of the course, a student will be able to:

- * Describe classic concepts, problems and key results in meta-complexity.
- * Analyze algorithms and cryptographic schemes related to meta-complexity

- * Explain reductions between meta-complexity and cryptographic problems .