ת.ז.: _____ מס' מחברת: _____

מבחן בקורס "מבוא לקריפטוגרפיה מודרנית"

סמסטר א' התשע"ד, מועד א'

תאריך: 21.1.2014

מרצה: פרופ' בני שור

מתרגל: ניר ביטנסקי

מומלץ לקרוא את כל ההנחיות והשאלות בתחילת המבחן, לפני תחילת כתיבת התשובות.

- משך הבחינה שלוש שעות.
- חומר עזר מותר: שני דפי A4, כתובים משני הצדדים.
- בראש כל עמוד בטופס המבחן יש למלא מספר ת"ז ומספר מחברת.
- במבחן ארבע שאלות פתוחות ולחלקן סעיפי משנה. כדי לקבל ציון 100 בבחינה יש לענות נכונה על כל השאלות. ניקוד כל סעיף מצוין לידו. אין בהכרח קשר בין ניקוד הסעיף ובין קושיו.
  - על התשובה לכל שאלה להופיע במסגרת המתאימה בטופס המבחן (טופס זה). יש לענות תשובות ברורות ותמציתיות. תשובות מסורבלות או לא ניתנות פיזית לקריאה יזכו לניקוד חלקי בלבד.
  - ודא/י היטב את תשובתך לפני כתיבתה בטופס המבחן. בסוף הטופס מצורפת מסגרת לשימוש במקרי "חירום".
  - מחברת הבחינה משמשת כטיוטא בלבד ולא תיבדק, אך יש להגישה עם המבחן.
- על סעיף של שאלה פתוחה ניתן לענות *"אינני יודע/ת"* כתשובה; על סעיף זה יינתנו 20% מהנקודות. במקרה זה אין להוסיף שום הסבר.
- מותר להשתמש בכל טענה שהוכחה בכיתה (בהרצאה, בתירגול או בתרגיל הבית) בתנאי שמצטטים אותה באופן מדויק. טענות שהוכחו במקום אחר (כגון: בספר הלימוד, בויקיפדיה, ב־MIT, בסמסטר קודם) יש להוכיח מחדש. בפתרון סעיף בשאלה מותר להשתמש בתוצאות הסעיפים הקודמים, גם אם לא פתרתם אותם.
- מומלץ לא להתעכב יתר על המידה על שום סעיף.

בהצלחה!

א1		ב1		ג1	
א2		ב2			
א3		ב3		ג4	
א4		ב4			