ת.ז: _____ מספר מחברת: _____

<u>מבחן בקורס "מבוא לקריפטוגרפיה מודרנית"</u>

סמסטר א' תשע"ז, מועד א'

תאריך: 30.1.2017

מרצה: פרופ' בני שור

מתרגלת: אורית מוסקוביץ'

<u>מומלץ לקרוא את כל ההנחיות והשאלות בתחילת המבחן, לפני תחילת כתיבת התשובות.</u>

- 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 חמש שאלות פתוחות ולחלקן 2 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 <u>בטופס המבחן</u> (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 <u>אין להוסיף שום הסבר</u>.
- מותר להשתמש בכל טענה שהוכחה בכיתה (בהרצאה, בתרגול 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.
- רמזים הניתנים בשאלות הינם בגדר המלצה, ואין חובה להשתמש בהם.
- <u>המבחן מנוסח בלשון נקבה מטעמי נוחות בלבד, אך מיועד לנשים וגברים כאחד.</u>

בהצלחה!

שאלה 1	שאלה 2	שאלה 3	שאלה 4	שאלה 5	ציון בחינה