



מבוא לקריפטוגרפיה מודרנית
מבחן סוף סמסטר - מועד א'

13 בפברואר, 2002

מרצה: בני שור

משך המבחן: 3 שעות **לא תינתן הארכה!!!**
מותר **דף יחיד** של חומר עזר.

יש לכתוב בצורה מסודרת ונקייה ובכתב ברור. תשובות לא ברורות לא תיבדקנה.
נא להקדיש את 10 הדקות הראשונות לקריאת כל השאלות והבנתן
מקום רב לתשובה אינו מעיד בהכרח שאנו מצפים לתשובה ארוכה.
בכל סעיף, התשובה "**אינני יודעת**" תזכה ב-20% מהניקוד.

שם משפחה:

שם פרטי:

מספר זהות:

ניקוד מירבי	ניקוד מבחן		
10	א	1	
10	ב		
10	ג		
10	ד		
10	ה		
10	א	2	
10	ב		
10	ג		
10	ד		
10	ה		
			ציון מבחן

בהצלחה !

ד (10 נקודות).

נתונים שני מפתחות שונים k_1, k_2 . קיימות שתי הודעות m_1, m_2 כך ש-
 $AES_{k_1}(m_1) = AES_{k_2}(m_2)$

סיווג:

הסבר:
