אוניברסיטת תל-אביב
בית הספר למדעי המחשב

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 **״איננני יודע/ת״** תזכה ב-20% מהניקוד.

שם משפחה:

שם פרטי:

מספר זהות:

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

בהצלחה !

<u>שאלה 1 (50 נקודות)</u>

בשאלה זו חמישה סעיפים שעניינם קיום התנגשויות ביחס ל-AES. בכל סעיף מופיע מאורע, ועליכם לסווג את ההסתברות שמאורע זה מתרחש על פי חמש הקטגוריות הבאות:

(1) בלתי אפשרי.
(2) אפשרי, אך בעל הסתברות זניחה (למשל 2^{-59}).
(3) סביר (למשל קורה בהסתברות 0.75 או בהסתברות e^{-1}).
(4) כמעט בטוח (למשל קורה בהסתברות $1-2^{-59}$).
(5) קורה תמיד.

בכל סעיף יש להוסיף הסבר קצר המסביר כיצד הגעתם לסיווג.
ניתן להניח הנחות "סבירות" לצורך ההסברים מבלי להוכיחן, אך יש לנסח אותן במפורש.
כל המפתחות k וההודעות m הם מחרוזות מאורך 128 מעל $\{0,1\}$.

א (10 נקודות).
נתון מפתח k. **קיימות** שתי הודעות **שונות** m_1,m_2 כך ש- $AES_k(m_1)=AES_k(m_2)$.

סיווג:

הסבר:

ב (10 נקודות).

נתונים שני מפתחות **שונים** k_1, k_2 . **קיימת** הודעה m כך ש- $AES_{k1}(m)=AES_{k2}(m)$.

סיווג:

הסבר:

ג (10 נקודות).

קיימים שני מפתחות **שונים** k_1,k_2 כך ש- $AES_{k1}(k_2)=AES_{k2}(k_1)$.

סיווג:

הסבר:

ד (10 נקודות).

נתונים שני מפתחות **שונים** k_1,k_2. **קיימות** שתי הודעות m_1,m_2 כך ש- $AES_{k1}(m_1)=AES_{k2}(m_2)$.

סיווג:

הסבר:

ה (10 נקודות).
נתונים שני מפתחות **שונים** k_1,k_2. **קיימת** הודעה m כך ש- $AES_{k1}(m)=AES_{k2}(m)$.

סיווג:

הסבר:

ו (10 נקודות).
נתונים שני מפתחות **שונים** k_1,k_2. שתי הודעות m_1,m_2 נבחרות באקראי.
מתקיים $AES_{k1}(m_1)=AES_{k2}(m_2)$.

סיווג:

הסבר:

<u>שאלה 2 (50 נקודות)</u>

בשאלה זו חמישה סעיפים שעניינם שדות סופיים Z_p וחוגים Z_N כאשר $N=pq$ ו-p,q ראשוניים.

א (10 נקודות).
יהי p מספר ראשוני המקיים $p = 3 \pmod 4$. הוכיחו כי $p-1$ אינו שארית ריבועית ב-Z_p^*.

ב (10 נקודות).
יהי p מספר ראשוני בתחום $2^{n-1} < p < 2^n$ המקיים $p = 3 \pmod 4$. תארו אלגוריתם דטרמיניסטי פשוט ויעיל (פולינומיאלי ב-n) להוצאת שורש ריבועי ב-Z_p^*.
האלגוריתם מקבל כקלט את p ואיבר $x \in Z_p^*$ ומחזיר או $y \in Z_p^*$ המקיים $y^2 = x \pmod p$ או את התשובה שאין ל-x שורש ריבועי מודולו p. הוכיחו **בקיצור** את נכונות האלגוריתם.

ג (10 נקודות).

יהיו p,q מספרים ראשוניים בתחום $2^{n-1} < p < 2^n$ המקיימים $p = 3 \pmod 4, q = 3 \pmod 4$, ויהי N=pq. תארו אלגוריתם דטרמיניסטי פשוט ויעיל (פולינומיאלי ב-n) להוצאת שורש ריבועי ב-Z_N^* **בהנתן הפרוק** של N.

האלגוריתם מקבל כקלט את p,q ואיבר $x \in Z_p^*$ ומחזיר כפלט או $y \in Z_p^*$ המקיים $y^2 = x \pmod N$ או את התשובה שאין ל-x שורש ריבועי מודולו N. הוכיחו **בקיצור** את נכונות האלגוריתם.

ניתן להניח קיום אלגוריתם יעיל להוצאת שורש ריבועי מודולו p ומודולו q .

ד (10 נקודות).
יהיו p,q מספרים ראשוניים המקיימים $p = 3 \pmod 4, q = 3 \pmod 4$, ויהי N=pq.

הראו כי אם $x \in Z_N^*$ ו- $x=y^2 \pmod N$ אז ל-x יש **ארבעה** שרשים ריבועיים שונים מודולו N: y_1, y_2, y_3, y_4 אשר מתוכם אחד בדיוק הוא עצמו שארית ריבועית מודולו N.

ניתן להסתמך על סעיף א (גם אם לא הוכחתם אותו).

ה (10 נקודות).
מערכת ההצפנה הבאה הינה גרסא של מערכת עם מפתח פומבי שהוצעה בספרות, המשתמשת אף היא באריתמטיקה של Z_N כאשר $N=pq$ ו-p,q ראשוניים. השימוש העיקרי של גרסא זו הוא לצורך החלפת מפתחות (**ולא** להצפנת טקסט).

יהיו p,q מספרים ראשוני בתחום $2^{n-1}< p < 2^n$ המקיימים $p = 3 \pmod 4, q = 3 \pmod 4$, ויהי $N=pq$.

מפתח פומבי: N.
מפתח פרטי: הפרוק של N: p ו- q.

מרחב ההודעות הוא אוסף השאריות הריבועיות מודולו N. (ניתן ליצור הודעה אקראית במרחב זה גם ללא ידיעת הפרוק של N על ידי בחירת איבר מתוך Z_N^* באקראי, והעלאתו בריבוע מודולו N).

הצפנה: $E(y)= y^2 \pmod N$.
פענוח: בהנתן שארית ריבועית $x \in Z_N^*$, הפענוח של x הינו $D(x)= y_i$ שהוא עצמו ריבוע מודולו N וגם שורש ריבועי של x מודולו N. על פי סעיף (ד) y_i זה אכן יחיד.

הראו כי ניתן לשבור מערכת זו ביעילות על ידי chozen ciphertext attack.

התוקף אמור ליצר מספר ciphertexts: $x_1,x_2,...x_m$ שהם כולם שאריות ריבועיות מודולו N, לקבל את m הפענוחים $D(x_1),D(x_2),...,D(x_m)$, ולמצוא את הפרוק של N (בהסתברות גבוהה).

רמז: אם s,r הם איברים שונים ב-Z_N^* כך ש-s שונה מ- $N-r$ וגם $s^2 \pmod N = r^2 \pmod N$, אז $1<gcd(s-r,N)<N$.

ו (10 נקודות).

יהי $N=pq$ ו-p,q ראשוניים גדולים. אבן הבנין הבסיסית של פרוטוקול הזיהוי שנדון בהרצאה היא העובדה הבאה: משתמש רוצה להוכיח כי הוא יודע שורש ריבועי של S מודולו N. המשתמש מוסר X (איבר מתוך Z_N^*). אחרי קבלת X המערכת שולחת למשתמש אתגר $b \in \{0,1\}$.

אם $b=0$ על המשתמש לספק שורש ריבועי של X מודולו N.
אם $b=1$ על המשתמש לספק שורש ריבועי של XS מודולו N.

הראו כיצד משתמש אשר אינו יודע שורש ריבועי של S מודולו N יכול לרמות, לו האתגר b היה נשלח אליו **לפני מסירת** X.