

**מבוא לקריפטוגרפיה מודרנית, סמסטר א' 2007/8**

בני שור ורני הוד

מבחן מועד א', 31/3/08

**הוראות**

1. מומלץ לקרוא את כל ההנחיות והשאלות בתחילת המבחן, לפני תחילת כתיבת התשובות.
2. משך הבחינה – שלוש שעות.
3. חומר עזר מותר: שני דפי פוליו (דו צדדיים) בלבד.
4. יש לענות על השאלות בטופסי הבחינה בלבד (מצד אחד של הדף). מחברות הבחינה ישמשו כטיוטה בלבד ולא ייקראו.
5. יש למלא בטופסי הבחינה ובמתברות את מספר ת.ז. שלכם.
6. ניקוד השאלות:
  - א. בבחינה ארבע שאלות "פתוחות": יש לענות על כולן.
  - ב. הניקוד לכל שאלה נע בין 20 ל-30 נקודות, ובכל אחת סעיפים שמשקלם מצויין.
  - ג. אין בהכרח קשר בין הניקוד וקושי הסעיפים.
  - ד. לכל סעיף, התשובה "אינני יודע/ת" מזכה ב-20% ממשקל הסעיף. במקרה זה אין להוסיף שום הסבר.
7. יש לדאוג שהבודקים יוכלו לקרוא את התשובות ללא שימוש במיקרוסקופ, תוכנה לזיהוי תוים, או פניה לבעלת אוב.
8. יש לענות תשובות ברורות ותמציתיות. תשובות מסורבלות וארוכות שלא לצורך עלולות לגרום הורדת נקודות.

**בהצלחה !**

	<b>שאלה 1</b>
	סעיף א'
	סעיף ב'
	סעיף ג'
	<b>שאלה 2</b>
	סעיף א'
	סעיף ב'
	<b>שאלה 3</b>
	סעיף א'
	סעיף ב'
	סעיף ג'
	<b>שאלה 4</b>
	סעיף א'
	סעיף ב'
	<b>סך הכל</b>

## שאלה 1 (20 נקודות) Message Authentication Codes

תהי  $E_k$  פונקציית הצפנה עם מפתח פרטי  $k$  בן  $n$  ביטים, הפועלת על בלוק בן  $n$  ביטים. נתאר שתי בניות מוצעות לאימות עם מפתח פרטי משותף. שתי הבניות דמויות CBC-MAC, אך שונות ממנו.

### (א) (10 נקודות)

הסכמה הבאה מוגדרת עבור הודעות בנות שני בלוקים בדיוק,  $m = m_1, m_2$ .

נגדיר  $t_0 = E_k(IV)$  כאשר  $IV$  הוא בלוק של  $n$  אפסים.

$$t_2 = E_k(t_1 \text{ XOR } m_2), \quad t_1 = E_k(t_0 \text{ XOR } m_1)$$

$$MAC_k(m_1, m_2) = (m_1, m_2, t_0, t_1, t_2)$$

(זה דומה ל-CBC-MAC, אך כאן מצפינים את  $IV$ , ומוציאים כחלק מן ה-MAC את תוצאות הביניים). הראו כיצד לזייף הודעה שטרם ראיתם. ניתן ל"מסור" מספר קטן של הודעות ולקבל את ה-MAC שלהן (כמובן, פרט להודעה שברצונכם לזייף).

(ב) 10 נקודות

הסכמה הבאה מוגדרת עבור הודעות בנות בלוק אחד,  $m=m_1$ , או שני בלוקים,  $m=m_1, m_2$ .

נגדיר  $t_1 = E_k(k \text{ XOR } m_1)$ , כאשר  $k$  המפתח הסודי,  $t_2 = E_k(t_1 \text{ XOR } m_2)$ .

$$\text{MAC}_k(m_1, m_2) = (m_1, m_2, t_2), \quad \text{MAC}_k(m_1) = (m_1, t_1)$$

(זה דומה ל-CBC-MAC, אך כאן IV הוא המפתח הסודי).

הראו כיצד לזייף הודעה שטרם ראיתם. ניתן ל"מסור" מספר קטן של הודעות ולקבל את ה-MAC שלהן

(כמובן, פרט להודעה שברצונכם לזייף).

## **שאלה 2 (30 נקודות)**

יהי  $n$  מספר טבעי בתחום שבין 100 ל-1000. נבחן את מערכת ההצפנה הבאה, בעלת מפתח פרטי. הטקסט שלנו מורכב ממשפטים באנגלית. הא"ב כולל אותיות ורווחים בלבד (ללא capital letters, מספרים, סימני פיסוק, וכו'). כמו כן נניח כי אורך הטקסט הוא כפולה שלמה של  $n$  (אחרת "נרפד" את סופו ברווחים), וכי אורך זה גדול מאוד. אנו מצפינים את הטקסט בשני שלבים. בשלב א' מפעילים על האותיות הצבה (סודית)  $S$ , כלומר תמורה מ-26 האותיות לעצמן. בשלב זה רווחים אינם משתנים. בשלב ב' מחלקים את הטקסט (אחר ההצבה) לבלוקים רציפים מאורך  $n$  תווים כל אחד. על כל בלוק מופעלת כעת תמורה  $P$  על המיקומים (מתוך חבורת התמורות על  $n$  עצמים).  $P$  מחליפה את מיקום האותיות והרווחים בתוך הבלוק. אותה תמורה  $P$  מופעלת על כל אחד מן הבלוקים.

תוצאת שלב ב' הוא הטקסט המוצפן.

### **(א) (10 נקודות)**

נניח כי  $n$  ידוע. המפתח הסודי הוא מטריצת ההצבה,  $S$ , ותמורת המיקומים,  $P$ . תארו התקפה המוצאת את את מטריצת ההצבה,  $S$  (כאשר  $P$  אינה ידועה). הסבירו האם התקפתכם יעילה – אין צורך בניתוח מדויק.

**(ב) 10 נקודות)**

נניח כי  $n$  ידוע, וכי פיתחתם התקפה שמצאה את מטריצת ההצבה,  $S$ . תארו התקפה המוצאת את תמורת המיקומים,  $P$ . הסבירו האם התקפתכם יעילה – אין צורך בניתוח מדויק.  
רמז: כדאי להשתמש בסטטיסטיקות ידועות על זוגות אותיות. למשל ש- $th$  הוא הזוג הנפוץ ביותר, או שאחרי  $q$  מופיע תמיד  $u$ .

**ג) (10 נקודות)**

נניח כעת כי  $n$  אינו נתון. המפתח הסודי הוא  $n$ , מטריצת ההצבה  $S$  ותמורת המיקום  $P$ . תארו התקפה המוצאת את המפתח הסודי. הסבירו את השוני בסיבוכיות ביחס לסעיף הקודם – אין צורך בניתוח מדויק.

### שאלה 3 (20 נקודות)

בוב משתמש ב-RSA לצורך החלפת מפתחות. הוא קנה חבילת תכנה אמינה אשר בה גדלי הראשוניים המיוצרים הם כאלו עבורם המודולוס  $m=pq$  הוא בן 1024 ביטים, לאחרונה קרא בוב (באתר [crypto-crack.org.ru](http://crypto-crack.org.ru)) טענות על פיהן RSA עם מודולוס  $m$  בן 1024 ביטים מתחיל להיות מסוכן (חשוף להתקפה). מאידך, התברר לבוב כי עקב השקעת כל הונו באגרות חוב מגובות משכנתאות מסוג sub-composite, אגרות חוב שערכן צלל לאחרונה, אין הוא מסוגל לעמוד במטלה הכספית הכרוכה בקניית חבילת התכנה המעודכנת.

בצר לו, החליט בוב לערוך בעצמו שדרוג, תוך שהוא ממשיך לעשות שימוש ב-RSA עם מודולים בני 1024 ביטים. בוב משתמש עתה בשני מודולים שונים אותם הוא מפרסם,  $m_3 > m_1$ , עם  $m_3 - 1 \mid m_1$ . לכל מודולוס מייצר בוב שני מפתחות הצפנה פומביים:  $e_1, e_2$  עבור  $m_1$ , ו-  $e_3, e_4$  עבור  $m_3$ . לכל מפתח הצפנה פומבי יש מפתח פיענוח פרטי המתאים לו.

כדי להצפין בלוק  $P$  אל בוב  $(P < m_1)$ , אהובה א' מחשבת תחילה  $C_1 = P^{e_1} \bmod m_1$

הצפנה שניה  $C_2 = C_1^{e_2} \bmod m_1$

הצפנה שלישית  $C_3 = C_2^{e_3} \bmod m_3$

הצפנה רביעית (אחרונה ודי)  $C = C_3^{e_4} \bmod m_3$ . זו ההודעה המוצפנת הנשלחת אל בוב.

נניח כי הזמן הנדרש לשבור את המערכת המקורית הוא  $T$  והזכרון הנדרש הוא  $S$ . במונח "לשבור" אנו מתכוונים למציאת שיטה המאפשרת פענוח יעיל, אך לא בהכרח למציאת הפרוק של  $m$  או שחזור מפתח הפענוח המקורי,  $d$ .

**(א) (10 נקודות)**

מהם הזמן והזיכרון הנדרשים לשבירת המערכת החדשה של בוב? נמקו את תשובתכם.



**(ב) 10 נקודות)**

האם בוב יכול היה להשיג תוצאות בטיחות דומות תוך שימוש במספר מפתחות קטן יותר (הסבירו אם כן או לא, ונמקו).

**שאלה 4** (30 נקודות)

**(א) (15 נקודות)**

יהיו  $p$  ו- $q$  מספרים ראשוניים אי זוגיים שונים. נתון כי  $g$  הוא איבר פרימיטיבי (יוצר כפלי) מודולו  $p$ , ו- $h$  הוא איבר פרימיטיבי (יוצר כפלי) מודולו  $q$ . הראו כי קיים איבר  $f$  בתחום  $[1..pq-1]$  כך ש- $f \bmod p$  הוא יוצר כפלי מודולו  $p$ , ו- $f \bmod q$  הוא יוצר כפלי מודולו  $q$ .

**תיקון:  $p$  ו- $g$  שניהם בני  $n$  ביטים,  $n > 10$ .**

**(ב) (15 נקודות)**

כפי שצויין (אך לא הוכח) בשיעור, בחוג  $Z_{pq}^*$  אין יוצרים כפליים. עדיין יש שם תת חבורות ציקליות רבות, ובהן בעיית הלוגריתם הדיסקרטי מוגדרת היטב. עבור  $f$  מחלק א', הראו כי בחוג  $Z_{pq}^*$  הלוגריתם של  $f^{pq} \pmod{pq}$  (בחזקת  $pq$  מודולו  $pq$ ) לפי בסיס  $f$  שווה  $p+q-1$ . שימו לב כי חלק מן ההוכחה צריך להיות שהלוגריתם אינו קטן מהגודל המבוקש  $p+q-1$ .  
(גם אם לא פתרתם את חלק א', תוכלו להניח כאן כי  $f$  כזה קיים, ולפתור את חלק ב').