

**המחלקה למדעי המחשב**

**דר' עמוס ביימל**

## **קריפטוגרפיה - מועד מיוחד**

**202-1-5351**

**סמסטר ב' תשס"ב**

**13.10.2002**

**הנחיות:**

1. בטופס הבחינה שני דפים מלבד דף זה.
2. בבחינה 3 שאלות שמשקלן אינו שווה. יש לענות על כולן.
3. הבחינה עם חומר פתוח.
4. נמקו את כל תשובותיכם. פתרון ללא הוכחה לא יתקבל.
5. משך הבחינה 3 שעות.
6. מומלץ לא להיתקע זמן רב מדי על שום סעיף.
7. הנכם רשאים להסתמך על סעיפים קודמים, גם אם לא השבתם עליהם.

**בהצלחה!**

## שאלה 1 [34 נקודות]

להזכירכם, במערכת החתימה RSA המפתח הפרטי הוא  $(N, d)$  והמפתח הציבורי הוא  $(N, e)$  כאשר  $N$  הוא מכפלה של שני ראשוניים גדולים ו- $ed \equiv 1 \pmod{\varphi(N)}$ . החתימה על מסמך  $M \in \mathbb{Z}_N$  היא  $M^d \pmod N$ . כפי שראינו בכיתה מערכת זו אינה עמידה להתקפת הודעה נבחרת בגלל התכונה הכיפולית של RSA (כלומר,  $((M_1)^d (M_2)^d \equiv (M_1 M_2)^d \pmod N)$ ). כדי להתגבר על תכונה זו הוצא לחתום על מסמך  $M$  על ידי  $(M+1)^d \pmod N$ .

### סעיף א [5 נקודות]

איך מוודאים בצורה יעילה שחתימה היא חוקית?

### סעיף ב [14 נקודות]

מערכת זאת אינה עמידה כנגד התקפת הודעה נבחרת. בהינתן מסמך  $M$ , מתקיף מגריל  $M_1 \in \mathbb{Z}_N^*$  בהתפלגות אחידה, מחשב  $M_2 \leftarrow (M+1)(M_1)^{-1} \pmod N$  ומבקש מהחותם החוקי לחתום על  $M_1 - 1$  ועל  $M_2 - 1$ . הראו איך המתקיף יכול בצורה יעילה לחשב חתימה על  $M$ .

### סעיף ג [15 נקודות]

הראו איך מתקיף יכול בצורה יעילה לחתום על מסמך נתון  $M$  בעזרת בקשה מהחותם החוקי לחתום על הודעה אקראית אחת.

## שאלה 2 [33 נקודות]

מחלק מחזיק שני סודות  $a, b \in \mathbb{Z}_p^*$  ומחלק אותם באופן בלתי תלוי על פי הסכמה של שמיר. כלומר, עבור ראשוני גדול המחלק בוחר  $r_1, \dots, r_{t-1}, q_1, \dots, q_{t-1}$  באקראי מתוך  $\mathbb{Z}_p^*$ , ומחשב לכל  $j$  את הערכים  $a_j \leftarrow (a + \sum_{i=1}^{t-1} r_i j^i) \pmod p$  ו-  $b_j \leftarrow (b + \sum_{i=1}^{t-1} q_i j^i) \pmod p$ .

### סעיף א [17 נקודות]

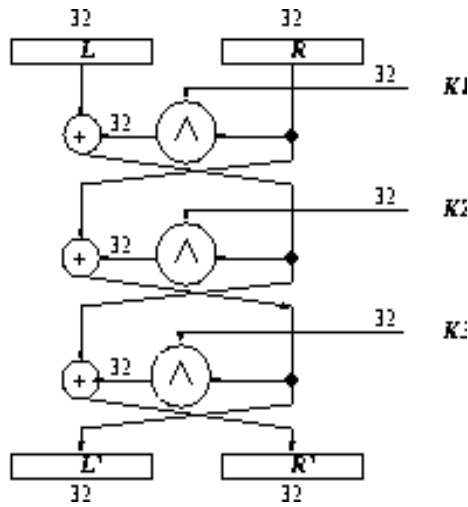
המחלק נותן למשתתף  $j$  את החלק  $(a_j + b_j) \pmod p$  לכל  $j$ . הוכיחו כי כל קבוצה של  $t$  משתתפים שתנסה לשחזר את הסוד מתוך החלקים שקיבלה כמו בסכמה של שמיר, תשחזר את הסוד  $(a+b) \pmod p$ .

### סעיף ב [16 נקודות]

המחלק נותן למשתתף  $j$  את החלק  $(a_j \cdot b_j) \pmod p$  לכל  $j$ . האם כעת כל קבוצה של  $t$  משתתפים שתנסה לשחזר את הסוד מתוך החלקים שקיבלה כמו בסכמה של שמיר, תשחזר את הסוד  $(a \cdot b) \pmod p$ ? נמקו תשובתכם.

### שאלה 3 [33 נקודות]

בשאלה זו נראה איך לשבור מערכת הצפנה דמוית DES עם 3 סיבובים כאשר הפונקציה  $f$  מוחלפת ב-  $\wedge$ , כלומר, מבצעים  $\wedge$  (AND) של כל ביט בנפרד. ליתר דיוק, נעסוק במערכת הקריפטוגרפית המצוירת לעיל.



#### סעיף א [6 נקודות]

מהו הפלט של המערכת על ההודעה  $M=(1^{32}, 0^{32})$ ?

#### סעיף ב [5 נקודות]

הראו כיצד איב יכולה בצורה יעילה למצוא את  $k_2$  על ידי התקפת הודעה נבחרת בשימוש בהודעה אחת.

#### סעיף ב [22 נקודות]

הראו כיצד איב יכולה בצורה יעילה ובהסתברות גבוהה למצוא את  $k_2$  על ידי התקפת הודעה אקראית? יש להשתמש במספר קטן ככל האפשר של הודעות אקראיות.  
תזכורת: בהתקפת הודעה אקראית המאזין מקבל זוגות של הודעה והצפנתה, כאשר כל הודעה נבחרת בהתפלגות אחידה מתוך מרחב ההודעות.