מס' ת.ז.

מבוא לקריפטוגרפיה מודרנית, סמסטר א' 2007/8

בני שור ורני הוד

מבחן מועד ב', 2/5/08

<u>הוראות</u>

1. **מומלץ לקרוא את כל ההנחיות והשאלות בתחילת המבחן, לפני תחילת כתיבת התשובות.**
2. משך הבחינה –**שעתיים וחצי.**
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 ובמחברות** את מספר ת.ז. שלכם\ן.
6. **מומלץ** לא להשתהות זמן רב מדי על שום שאלה או סעיף בודד.
7. ניקוד השאלות
   א. בבחינה שלוש שאלות "פתוחות": יש לענות על **כולן**.
   ב. הניקוד לכל שאלה נע בין 30 ל-40 נקודות, ובכל אחת סעיפים שמשקלם מצויין.
   ג. אין בהכרח קשר בין הניקוד וקושי הסעיפים.
   ד. לכל סעיף, התשובה "**איננ**י **יודע/ת**" מזכה ב-20% ממשקל הסעיף. במקרה זה **אין להוסיף** שום הסבר.
   ה. מומלץ שלא להקדיש לשום סעיף בודד זמן רב מדי.
8. יש לדאוג שהבודקים יוכלו לקרוא את התשובות ללא שימוש במיקרוסקופ, תוכנה לזיהוי תוים, או פניה לבעלת אוב.
9. יש לענות תשובות ברורות ותמציתיות. תשובות מסורבלות וארוכות שלא לצורך עלולות לגרור הורדת נקודות.
10. בשאלה 1, סעיף ב' תלוי בפתרון למשוואה מסעיף א'. אם שוכנעתם כי אינכם מצליחים לפתור את סעיף א' ורשמתם "**איננ**י **יודע/ת**", תוכלו לקבל את הפתרון למשוואה מהמרצה. החלטה זו אינה הפיכה (כלומר הניקוד לסעיף א' בבדיקה לא יהיה גבוה מ-3 נקודות).

בהצלחה !

שאלה 1	
סעיף א'	
סעיף ב'	
שאלה 2	
סעיף א'	
סעיף ב'	
סעיף ג'	
שאלה 3	
סעיף א'	
סעיף ב'	
סך הכל	

<u>שאלה 1</u> (30 נקודות) הטלת מטבע בטלפון.

אהובה א' מפרסמת מספר ראשוני p כך ש-3 אינו מחלק את p-1.
כן היא מפרסמת את הפרוק המלא של p-1, ושני יוצרים כפליים (איברים פרימיטיביים) שונים ב-Zp, g ו-h.

ברוך ב' מוודא כי כל המספרים שאהובה מפרסמת הם מהצורה הנכונה. כלומר ש-p אכן ראשוני, ש-3 אינו מחלק את p-1, כי הפרוק הנתון של p-1 נכון ומלא, את העובדה ש-g ו-h שונים, וכי שניהם פרימיטיביים. (נזכיר כי בהינתן הפרוק של p-1, ניתן לבדוק ביעילות האם איבר נתון הוא יוצר כפלי.)

כעת מבצעים שניהם את הטלת המטבע הבאה:
אהובה בוחרת (באופן שרירותי) x ו-y בתחום $0\leq x,y\leq p-2$.
היא שולחת לברוך את המספרים $z=g^x h^y \bmod p$, $t=g^x g^y \bmod p$
ברוך מנחש האם $y \bmod (p-1)$ הוא בתחום $[0 .. (p-1)/2]$ או בתחום $[(p+1)/2 .. p-2]$.
הוא שולח את הניחוש לאהובה.
אהובה חושפת x',y' המתאימים ל-t,z, ששלחה (כלומר, $z=g^{x'} h^{y'} \bmod p$, $t=g^{x'} g^{y'} \bmod p$).

אם הניחוש של ברוך מתקיים לגבי y' שנחשף, הוא מנצח. אחרת הוא מפסיד.

מטרת השאלה היא להראות כי אהובה יכולה לנצח **תמיד** (גם אם היא מוגבלת לחישובים יעילים בלבד).

א) (15 נקודות)

יהי p מספר ראשוני אי זוגי כך ש-3 אינו מחלק את p-1. יהיו a,b בתחום $0\le a,b\le p-2$, כך שההפרש a-b הוא זוגי. הראו כי למערכת המשוואות (שתיהן (mod p-1 במשתנים x,y

$$x+y=a \bmod (p-1),\quad x+3y=b \bmod (p-1)$$

יש **שני** פתרונות שונים בתחום $0\le x,y\le p-2$.

עליכם להראות מהם הפתרונות וכיצד הם נמצאו.

ב) (15 נקודות)

הוכיחו כי אהובה יכולה לנצח **תמיד** במובן החזק הבא: **לכל בחירה** של x ו-y, ולכל ניחוש של ברוך, תוכל אהובה למצוא x',y' המתאימים ל-z,t ששלחה

(כלומר, $t=g^{x'}g^{y'} \bmod p$, $z=g^{x'}h^{y'} \bmod p$), ועבורם $y' \bmod (p-1)$ **אינו** בקטע שבחר ברוך.

רמז: ניתן לבחור $h=g^3 \bmod p$. אם זו בחירתכם, ולא פתרתם את חלק א', ראו הערה 10 בדף ההוראות.

<u>שאלה 2</u> (40 נקודות) one and two time pad.

פרופ' שור נחשף בחופשת הפסח ל"ספר מגוחך" של דודו גבע, עליו השלום, וקובי ניב, יבדל לחיים ארוכים (אדם, מוציאים לאור, י-ם, 1981). שבו את ליבו במיוחד עלילות יוסף (מחלקת המים, עיריית תל-אביב) והתובנות החבויות בהן. הוא החליט לחלוק שני פרקים שונים עם מר הוד, המתרגל. הספר מכיל עשרים פרקים קצרים של עלילות יוסף. כל אחד מן הפרקים הוא באורך 200 אותיות. האותיות לקוחות מאלף-בית בגודל 30 (22 אותיות עבריות, 5 אותיות סופיות, נקודה, פסיק, ורווח). חשיפת יתר לחידות וצפנים גרמה לפרופ' שור לשלוח את שני הפרקים כשהם מוצפנים בעזרת one time pad מאותו אלף-בית, באורך 400, אשר הוחלף באופן חשאי עם מר הוד ערב חופשת הפסח. ידוע לכם כי כל אחת משתי ההודעות מצפינה פרק כנ"ל, וכמו כן יש לכם גישה לספר. (בהצפנה מסוג זה עובדים אות אות ולא ביט ביט.)

א) (10 נקודות)

אתם מעוניינים לגלות מהם הפרקים שכה הפעימו את המרצה. מה הסיכוי שתצליחו במשימה? נמקו **בקיצור**.

ב) (20 נקודות)

עקב עודף צריכה של יין ומצות, מתברר כי במקום להשתמש ב-one time pad באורך 400, השתמש פרופ' שור **פעמיים** באותו one time pad באורך 200 (פעם אחת לכל פרק). הסבירו כיצד לנצל עובדה זו כדי לזהות את זוג הפרקים שנשלחו.

ג' (10 נקודות)

הניחו כי כל אחד מן הפרקים הוא מחרוזת אקראית מאורך 200 מעל האלף בית הנ"ל, וכי מחרוזות שונות הן בלתי תלויות. העריכו את הסיכוי שיהיה יותר מזוג אחד של פרקים המתאים לזוג המחרוזות המוצפנות שנשלחו בתנאים של סעיף ב'.

<u>שאלה 3</u> (30 נקודות) פונקציות ערבול קריפטוגרפיות hash functions

נתונה פונקציה $g:\{0,1\}^{2n} \rightarrow \{0,1\}^{n}$ עבור n קבוע וגדול למדי (נניח n=256). ידוע כי לא ניתן למצוא באופן יעיל התנגשויות עבור הפונקציה g.

נגדיר פונקציית ערבול H על הודעות M שארכן הוא כפולה שלמה של n (ולפחות פעמיים):

נסמן M=m_1 m_2 m_3…m_k כאשר כל m_i הוא מאורך n, ו-k גדול מ-1.

נסמן v_1=g(m_1 m_2)

v_2=g(v_1 m_3)

v_k=g(v_(k-1) m_k)

H(M)=v_k

א' (15 נקודות)

הראו כיצד למצוא ביעילות התנגשויות בפונקציה H.

ב' (15 נקודות)

נניח כי M היא מאורך 4n (ארבעה בלוקים). מה המספר הממוצע (על פני בחירת M) של M' מאורך 2n כך ש$H(M)=H(M')$? מהי השיטה היעילה ביותר שביכולתכם למצוא אשר על קלט M מאורך 4n מוצאת M' מאורך 2n כך ש$H(M)=H(M')$? תארו **בקצרה** את השיטה ואת סיבוכיותה.