ת.ז.: _____ מס' מחברת: _____

מבחן בקורס "מבוא לקריפטוגרפיה מודרנית"

סמסטר א' התש"ע, מועד ב'

תאריך: 5.3.2010

מרצה: פרופ' בני שור

מתרגל: רני הוד

מומלץ לקרוא את כל ההנחיות והשאלות בתחילת המבחן, לפני תחילת כתיבת התשובות.

- משך הבחינה שלוש שעות.
- חומר עזר מותר: שני דפי A4, כתובים משני הצדדים.
- בראש כל עמוד בטופס המבחן יש למלא מספר ת"ז ומספר מחברת.
- במבחן ארבע שאלות פתוחות ולחלקן סעיפי משנה. כדי לקבל ציון 100 בבחינה יש לענות נכונה על כל השאלות. ניקוד כל סעיף מצוין לידו. אין בהכרח קשר בין ניקוד הסעיף ובין קושיו.
  - על התשובה לכל שאלה להופיע במסגרת המתאימה בטופס המבחן (טופס זה). יש לענות תשובות ברורות ותמציתיות. תשובות מסורבלות או לא ניתנות פיזית לקריאה יזכו לניקוד חלקי בלבד.
  - ודא/י היטב את תשובתך לפני כתיבתה בטופס המבחן. בסוף הטופס מצורפת מסגרת לשימוש במקרי "חירום".
  - מחברת הבחינה משמשת כטיוטא בלבד ולא תיבדק, אך יש להגישה עם המבחן.
- על סעיף של שאלה פתוחה ניתן לענות *"אינני יודע/ת"* כתשובה; על סעיף זה יינתנו 20% מהנקודות. במקרה זה אין להוסיף שום הסבר.
- מותר להשתמש בכל טענה שהוכחה בכיתה (בהרצאה, בתירגול או בתרגיל הבית) בתנאי שמצטטים אותה באופן מדויק. טענות שהוכחו במקום אחר (כגון: בספר הלימוד, בויקיפדיה, ב־MIT, בסמסטר קודם) יש להוכיח מחדש. בפתרון סעיף בשאלה מותר להשתמש בתוצאות הסעיפים הקודמים, גם אם לא פתרתם אותם.

בהצלחה!

א1		ב1						
א2		ב2		ג2		ד2		
א3		ב3		ג3				
א4		ב4		ג4				

ת.ז.: _____ מס' מחברת: _____

שאלה 1 (20 נק')

יהי p מספר ראשוני מהצורה $p = 8k + 5$ (k טבעי).

סעיף א' (10 נק')

הראו כי -1 הוא שארית ריבועית ב-$\mathbb{Z}_p^*$, קרי יש $b \in \mathbb{Z}_p^*$ עבורו $b^2 = -1 \bmod p$.

הוכחה:

סעיף ב' (10 נק')

נתון a המהווה שארית *ריבועית* ב-$\mathbb{Z}_p^*$, כלומר $a = x^4 \bmod p$ עבור $x \in \mathbb{Z}_p^*$ כלשהו. רני רוצה לחשב שורש *ריבועי* של a ובני הציע לו לחשב $r = a^m \bmod p$ עבור m כלשהו. האם בהכרח יש m טבעי עבורו $a^m = \pm x^2$? הוכיחו או תנו דוגמא נגדית.

הוכחה/דוגמא נגדית:

שאלה 2 (20 נק')

<u>מערכת ElGamal – תזכורת:</u>
בוחרים p ראשוני מהצורה $p = 2q + 1$ ויוצר g של $\mathbb{Z}_p^*$; אלה ידועים לכל.
המפתח הפרטי הוא $0 \leq x < p - 1$ והמפתח הפומבי הוא $\beta = g^x$.
כדי להצפין את ההודעה m בוחרים $0 \leq k < p - 1$ אקראי ומחזירים את $(g^k \bmod p, m\beta^k \bmod p)$.
כדי לפענח את ההודעה (a, b) מחשבים $b \cdot a^{-x} \bmod p$.

שחקני הטניס גייל וג'יימס משתמשים במערכת ElGamal כדי לשלוח הודעות מוצפנות דרך הטלפון הסלולרי אל מאיר. באמתחתם מטבע שנקל הוגן המשמש כדי לייצר את הביטים האקראיים הדרושים להצפנה.

במהלך שהותם בנסיכות נפט מרוחקת אבד להם המטבע ועל כן הם נאלצו לייצר את המספרים האקראיים $k_1, k_2, \ldots, k_{100}$ (המשמשים בהתאמה להצפנת ההודעות $m_1, m_2, \ldots, m_{100}$) בשיטה הבאה:

- k_1 הוא מספר אקראי לחלוטין שאותו הספיקו לייצר מבעוד מועד;
- לכל $i \geq 2$ מחשבים את $k_i = 2k_{i-1} + 1 \bmod (p - 1)$.

דאחי חלפאן מאזין לתקשורת באופן פאסיבי. הוא יודע לפי פרסומים זרים את p, g, β. לאחר שמצא את המטבע על המגרש, עלו בו החשדות הבאים:

1. המספרים k_i אינם אקראיים.
2. ההודעות m_1 ו-m_6 זהות, כנראה בגלל הלחץ בו היו שרויים גייל וג'יימס במערכה השלישית.

עבור כל אחת מהתהיות להלן, אם התשובה חיובית, הוכיחו אותה ואם התשובה שלילית, נמקו בקצרה מדוע (במקרה זה אינטואיציה תספיק).

סעיף א' (5 נק')

האם ניתן לוודא את החשד שהמספרים $\{k_i\}$ יוצרו בשיטה שתוארה לעיל?

תשובה: כן / לא **הוכחה/נימוק:**

סעיף ב' (5 נק')

האם ניתן לפענח את כל ההודעות $m_1, m_2, \ldots, m_{100}$? (בהנחת $m_1 = m_6$ ושיטת ייצור ה-$\{k_i\}$)

תשובה: כן / לא **הוכחה/נימוק:**

סעיף ג' (5 נק')

האם ניתן לשחזר את המספר האקראי k_1 ? (בהנחת $m_1 = m_6$ ושיטת ייצור ה-$\{k_i\}$)

תשובה: כן / לא
הוכחה/נימוק:

סעיף ד' (5 נק')

האם ניתן לשחזר את המפתח הפרטי x של מאיר? (בהנחת $m_1 = m_6$ ושיטת ייצור ה-$\{k_i\}$)

תשובה: כן / לא
הוכחה/נימוק:

שאלה 3 (סה"כ 30 נק')

ר' שלום שבזי מצפין את מילות פיוטיו באמצעות מצפין בלוקים של 320 ביט בשם "חמדת ימים".

לחמדת ימים שלושה מפתחות, נסמנם K_0, K_1, K_2, בגודל 40 ביט כ"א.

המצפין משתמש בפונקציה $f : \{0,1\}^{160} \times \{0,1\}^{40} \to \{0,1\}^{160}$ המוגדרת ע"י $f(x,y) = \mathrm{SHA1}(xy)$, קרי הפעלת הפונקציה החד־כיוונית SHA1 על השרשור של x ו-y.

חמדת ימים מורכב משלושה סיבובים של רשת פייסטל. בלוק הקלט P מחולק לשני חצאים L_0, R_0 בגודל 160 ביט כ"א; בסיבוב ה-t מייצרים את $L_t = R_{t-1}$ ואת $R_t = L_{t-1} \oplus f(R_{t-1}, K_{t-1})$. בלוק הפלט C הוא השרשור של החצאים L_3, R_3.

סעיף א' (5 נק')

הגדרה זו של רשת פייסטל שונה מעט מזו שראינו בכיתה. הראו כיצד ניתן לפענח בלוק מוצפן בהנתן המפתחות K_0, K_1, K_2.

תשובה:

סעיף ב' (10 נק')

בחפירות ארכיאולוגיות בתימן נתגלה קובץ פיוטים חדש, מוצפן כולו ע"י חמדת ימים עם מפתחות לא ידועים (אותם מפתחות לכל הפיוטים בקובץ). מאחר והרב תכנן לשלוח פיוטים אלה לתחרות הפיוט הקצר של עיתון "הארץ", ניתן להסיק כי הם קצרים במיוחד (לא יותר מ-250 ביטים כ"א).[1]

הניחו כי המפענחים הם משוללי כל ידע בלשני או ספרותי, ועל כן אינם יכולים לזהות האם רצף גלוי נתון של 250 ביטים הוא פיוט תקין או לאו; האם ניתן בכלל לשחזר את המפתחות ואת הפיוטים? אם כן, כמה פיוטים מוצפנים נדרשים לשחזור מוצלח (בהסתברות גבוהה) בהנחה שהמפענחים אינם מוגבלים חישובית?

תשובה (מחקו את המיותר): לא ניתן / כן ניתן, ומספר הפיוטים הנדרשים הוא _____
נימוק:

[1] תזכורת: אם אורך ההודעה אינו כפולה שלמה של גודל הבלוק, מוסיפים תוים נוספים בסופה (במקרה שלנו, אפסים) עד שאורכה מהווה כפולה שלמה של גודל הבלוק ורק אז מצפינים.

סעיף ג' (15 נק')

בעקבות זכייתו של הרב בתחרות, התפרסם במלואו הטקסט של אחד מבין הפיוטים המוצפנים, קרי: יש בידינו זוג (P, C) שהוצפן ע"י חמדת ימים עם המפתחות הלא ידועים (בלוק אחד).

הראו כיצד ניתן לשחזר ביעילות את שלושת המפתחות.

תשובה:

שאלה 4 (סה"כ 30 נק')

נגדיר סכמת t מתוך n לחלוקת סוד *באופן חלש* באופן הבא. הסוד S הוא מספר בתחום $M \leq S < 2M$ (עבור פרמטר M). ברצוננו שכל קבוצה בת לפחות t משתתפים תוכל לשחזר את הסוד בהצלחה, אך לכל קבוצה בת לכל היותר $t-1$ משתתפים תהיה אי־ודאות מסוימת לגבי הסוד.[2]

להלן סכמת חלוקת סוד באופן חלש המבוססת על משפט השאריות הסיני (CRT). יהיו n מספרים ראשוניים $p_1 < p_2 < \cdots < p_n$. עבור סוד S, החלק שמקבל משתתף i הוא $S \bmod p_i$. כדי לשחזר את הסוד, קבוצת המשתתפים I משתמשת ב-CRT כדי לחשב את $S \bmod \prod_{i \in I} p_i$.

סעיף א' (10 נק')

מצאו תנאי מספיק (על $\{p_i\}_{i=1}^{n}, t, n, M$) כך שכל קבוצה בת t או יותר משתתפים תצליח בוודאות לשחזר את הסוד S. הסבירו בקצרה.

תנאי:
הסבר:

[2] כאן טמון ההבדל מסכמת חלוקה סוד רגילה, בה אסור אפילו שקבוצה קטנה תקבל מידע חלקי על הסוד. בסכמה החלשה דורשים רק שעבור כל $t-1$ חלקים של הסוד תהיינה לפחות *שתי* אפשרויות עקביות לערך S.

סעיף ב' (10 נק')

מצאו תנאי מספיק (על $\{p_i\}_{i=1}^{n}, t, n, M$) כך שתהיה זו סכמת חלוקת סוד באופן חלש, קרי שכל קבוצה בת פחות מ-t משתתפים לא תצליח לשחזר בוודאות את הסוד S. הסבירו בקצרה.

תנאי:
הסבר:

סעיף ג' (10 נק')

תנו דוגמא לפרמטרים t, n, M עבורם לא קיימת סכמת t מתוך n לחלוקת סוד באופן חלש המבוססת על CRT. הסבירו בקצרה.

דוגמא:
הסבר:

מסגרת "חירום" לשאלה מספר _____, סעיף _____:

מסגרת "חירום" לשאלה מספר _____, סעיף _____: