אוניברסיטת בן-גוריון בנגב
Ben-Gurion University of the Negev

המחלקה למדעי המחשב

דר' עמוס ביימל

קריפטוגרפיה - מועד ב'

202-1-5351

סמסטר ב' תשס"ב

1.8.2002

(כולל תיקונים בזמן המבחן)

הנחיות:

1. בטופס הבחינה שני דפים מלבד דף זה. ודאו כי כולם נמצאים בידכם.
2. בבחינה 4 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 [25 נקודות]

בשאלה זו נדון בסכמות לחלוקת סוד שבהם המעבדים ינסו לגלות אם אחד המעבדים מרמה.

סעיף א [10 נקודות]

מחלק מחזיק סוד $s \in \{0,1\}$ ומחלק אותו על פי הסכמה לחלוקת סוד של שמיר 2-מתוך-2. כלומר, בוחר r באקראי מתוך $\mathbb{Z}_p$ עבור $p > 2$ ראשוני גדול, והחלק של מעבד j הוא $(rj + s) \bmod p$ עבור $j \in \{1,2\}$. שימו לב כי p הוא ראשוני גדול אבל ישנם שני סודות אפשריים. נתון כי מעבד 1 יודע כי הסוד הוא 0. הראו איך מעבד 1 יכול לשנות את החלק שלו כך שהסוד המשוחזר יהיה 1.

סעיף ב [15 נקודות]

נשנה כעת את הסכמה מסעיף א. המחלק כעת בוחר r באקראי מתוך $\mathbb{Z}_p$ ו- x_1, x_2 באקראי מתוך $\mathbb{Z}_p^*$ עבור $p > 2$ ראשוני גדול, כאשר $x_1 \neq x_2$. החלק של משתתף j הוא $\langle x_j, (rx_j + s) \bmod p \rangle$ עבור $j \in \{1,2\}$. נתון כי מעבד 1 יודע כי הסוד הוא 0. הראו כי לא משנה איך מעבד 1 ינסה לשנות את החלק שלו, הסיכוי שהסוד המשוחזר יהיה 1 הוא לכל היותר $1/(p-2)$.

שאלה 2 [34 נקודות]

בשאלה זו נראה בעייתיות של מערכת ההצפנה RSA כאשר משתמשים ב- $e=3$ להצפין. יהי $N=pq$ מספר בין n ביטים שהוא מכפלה של שני ראשוניים גדולים כאשר $p < q < 2\sqrt{N}$ ו- $\gcd(3, \varphi(N)) = 1$. המפתח הציבורי הוא $(N,3)$ והמפתח הפרטי הוא (N,d) כאשר $3 \cdot d \equiv 1 (\bmod \varphi(N))$, כלומר קיים שלם A כך ש- $3d = A\varphi(N) + 1$.

סעיף א [5 נקודות]

הוכיחו כי $1 \leq A \leq 2$.

סעיף ב [7 נקודות]

הוכיחו כי $A \neq 1$. הסתמכו על העובדה כי $p > 3$ ולכן 3 לא מחלק את p ואת q.

סעיף ג [6 נקודות]

הראו איך לחשב בזמן $O(n)$ את d בהינתן $\varphi(N)$ ו- N.

סעיף ד [3 נקודות]

הראו כי $N - 4\sqrt{N} < \varphi(N) < N$.

סעיף ה [7 נקודות]

הראו איך איב, שיודעת מהו N, יכולה למצוא בצורה יעילה d' כך ש- $|d - d'| < 3\sqrt{N}$. שימו לב: איב אינה יודעת מהו $\varphi(N)$.

סעיף ו [6 נקודות]

הראו איך איב, שיודעת מהו N, יכולה למצוא את d על ידי $O(\sqrt{N})$ פתרונות של משוואות ריבועיות מעל הממשיים.

שאלה 3 [20 נקודות]

יהי (p,g,B) המפתח הציבורי של בוב במערכת ההצפנה של El-Gamal, ו- (p,g,b) המפתח הפרטי שלו. בוב מעוניין להעניק לשני חבריו יכולת לפענח את הודעותיו אם ישתפו פעולה. לשם כך, הוא מגריל $b_1 \in \mathbb{Z}_{p-1}$ באקראי ובהתפלגות אחידה ומחשב $b_2 \leftarrow (b-b_1) \bmod (p-1)$. בוב נותן לחבר הראשון את המפתח (p,g,b_1) ולחבר השני את המפתח $(p,2,b_2)$.

סעיף א [4 נקודות]

הסבירו מדוע כל חבר בנפרד אינו יכול לפענח הודעות שנשלחו לבוב.

סעיף ב [12 נקודות]

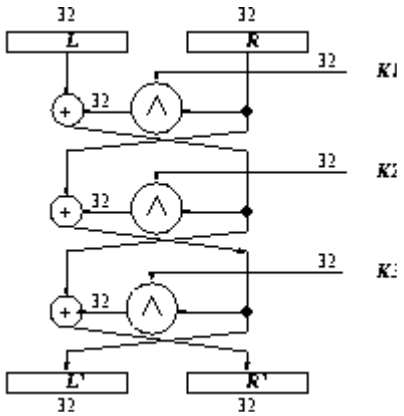
יהי $a \in \mathbb{Z}_{p-1}$ ו- $A \leftarrow g^a \bmod p$. הראו כיצד שני החברים היודעים את A יכולים ביחד לחשב בצורה יעילה את $A^b \bmod p$ מבלי לחשוף את המפתח הפרטי שלהם אחד לשני. הוכיחו תשובתכם על סמך ההנחה שהמערכת להחלפת מפתחות של Diffie&Hellman היא בטוחה. זכרו כי כל אחד מהחברים יודע מהו המפתח הציבורי של בוב.

סעיף ג [4 נקודות]

תהי (A,S) קריפטוגרמה שהוצפנה על ידי המפתח (p,g,B). הראו כיצד שני החברים יכולים ביחד לפענח בצורה יעילה את הקריפטוגרמה מבלי לחשוף את המפתח הפרטי שלהם אחד לשני.

שאלה 4 [26 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 [4 נקודות]

האם הפונקציה המחושבת על ידי המערכת היא חד-חד ערכית ועל?

סעיף ב [6 נקודות]

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

סעיף ג [6 נקודות]

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

סעיף ד [10 נקודות]

הראו כיצד איב יכולה בצורה יעילה למצוא את $k2$ על ידי התקפת הודעה נבחרת.