

מבוא לקריפטוגרפיה (203.3444/203.4444)

סמסטר אביב 2010 – מועד ב'
(אחרי תיקונים מהמבחן)

תאריך: 12.7.2011

מרצה: ד"ר אור דונקלמן

1. משך המבחן שעתיים וחצי.
2. במבחן 3 שאלות, ענה/י על כולן.
3. חומר עזר מותר בשימוש: כל חומר עזר מודפס. אין להשתמש בכל חומר עזר אלקטרוני.
4. הקדש/י את 10 הדקות הראשונות לקריאת כל השאלות והבנתן.
5. ענה/י תשובות קצרות וברורות ככל האפשר. נמק/י את תשובתך.
6. באם אינך יודע/ת את התשובה לסעיף, ניתן לרשום "לא יודע/ת", ולקבל כ-20% מציון הסעיף.

בהצלחה!

שאלה 1 (35 נקודות)

בשאלה זו נדון בהרצת פרוטוקול Diffie-Hellman מעל חבורה כללית.

א. הראה/י חבורה אחת בת יותר מ- 2^{150} איברים עבורה בעית הלוגריתם הדיסקרטי היא קלה, וחבורה אחת עבורה נחשבת הבעיה קשה. (5 נק')

תהי G חבורה בה בעית הלוגריתם הדיסקרטי נחשבת קשה, ויהי $g \in G$ יוצר שלה. בהמשך השאלה, כל הכפלים מבוצעים בתוך החבורה G .

ב. הראה/י אלגוריתם יעיל לחישוב g^x ב- G (בעל סיבוכיות מקסימלית של $O(\log x)$ כפלים ב- G). (5 נק')

לאחר קביעת g ו- G , כל משתמש U במערכת בוחר $X_U \in G^*$ באקראי ובאופן אחיד, ומחשב את $Y_U = g^{X_U}$ ומפרסם את Y_U בקובץ מרכזי במערכת הזמין לכל המשתמשים.

ג. הסבר/י כיצד A ו- B יכולים להסכים על מפתח סודי משותף תוך שימוש בידע הסודי שלהם והקובץ המרכזי. (5 נק')

ד. לאחר בחירת G , התגלה אלגוריתם הסתברותי A המסוגל לפתור את בעית האלגוריתם הדיסקרטי בחבורה G בהסתברות $1/500$ (כלומר בהנתן g^x ו- G , האלגוריתם מחזיר את x בהסתברות $1/500$). הסבר/י כיצד ניתן לפתור את בעית הלוגריתם הדיסקרטי ב- G לכל ערך g^x (באופן בלתי תלוי באופן פעולת A) בסיכוי של 75%. (6 נק')

כדי לשפר את ביצועי החישובים של העלאה בחזקה, הוחלט להשתמש בחבורה $G = Z_n^*$ כאשר n הינו כפולה של 100 המספרים הראשוניים הראשונים האי-זוגיים, כלומר $n = 3 * 5 * 7 * \dots * 547$. יהי $g \in G$ איבר מסדר גבוה (של לפחות 2^{150}).

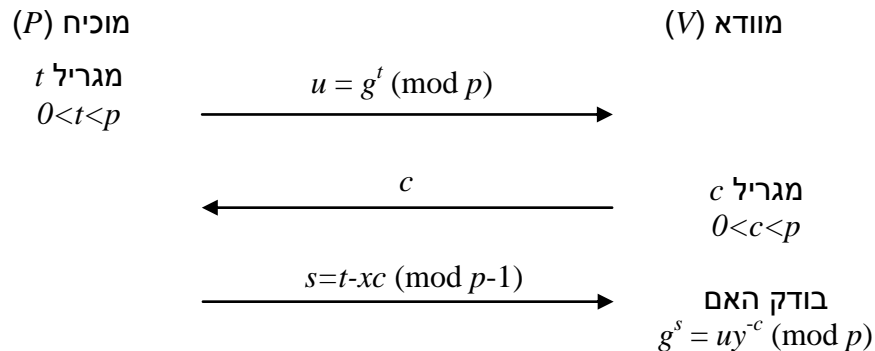
ה. הראה/י כיצד ניתן לחשב את $g^x \pmod{n}$ בצורה יעילה ככל האפשר. (7 נק')

ו. האם בעית הלוגריתם הדיסקרטי בחבורה זו היא בעיה קשה? אם כן, הסבר/י מדוע, או הסבר/י כיצד למצוא את הלוגריתם הדיסקרטי של איבר ב- G בהנתן g (אם קיים). (7 נק')

שאלה 2 (35 נקודות)

שאלה זו דנה באלגוריתם הזיהוי של Schnorr. בשיטה זו נבחר ראשוני גדול p ויוצר $g \in \mathbb{Z}_p^*$, שניהם משותפים לכל משתמשי המערכת. בשלב האיתחול, בוחר כל משתמש ערך x (כך ש- $0 < x < p$), ומפרסם את $y = g^x \pmod{p}$ (כמובן ש- x נשמר בסוד).

כאשר משתמש רוצה להוכיח את זהותו, מורץ הפרוטוקול הבא בין המשתמש (כמוכיח P) והמוודא (V):



- א. הראה/י כי הפרוטוקול הוא שלם (כלומר, משתמש היודע את x יכול להוכיח את זהותו בהצלחה). (5 נק')
- ב. הראה/י כי הפרוטוקול הוא נאות (כלומר משתמש שאינו יודע את x אינו יכול להצליח בפרוטוקול בסיכוי שהוא לא זניח). (5 נק')
- ג. ניח כי מתחזה ל- P , מצליח לגלות מה הערך c שישלח לו בהודעה השניה בפרוטוקול עוד לפני שהוא שולח את ההודעה הראשונה. הראה/י כיצד הוא יכול לנצל ידע זה לצורך התחזות מוצלחת גם ללא ידיעת x . (7 נק')

כדי להוכיח שהפרוטוקול הינו פרוטוקול אפס-ידע, הוצע הסימולטור הבא:

1. הסימולטור פולט את (p, g, y) .
2. בכל איטרציה מבצע הסימולטור את הצעדים הבאים:
 - a. מגריל t ושולח את $u = g^t \pmod{p}$ למוודא V^* .
 - b. עונה את התשובה c בהתאם ל- u .
 - c. הסימולטור משרשר למראה את הערכים הרלוונטיים בהתאם לסעיף ג'.
- ד. הסבר/י מדוע הסימולטור הנ"ל איננו מייצר מראה שמתפלג באופן דומה למראה המתקבל בעת הרצת הפרוטוקול האמיתי בין P ל- V^* . (7 נק')

סטודנט בקורס, הציע לשנות את תשובת המוכיח (ההודעה השלישית) ל- $s = x - tc \pmod{p-1}$.

- ה. הסבר/י כיצד מתבצעת הבדיקה של המוודא שאכן המוכיח יודע את x . (5 נק')
- ו. הסבר/י כיצד מוודא רמאי יכול להשיג את ערך x מתוך התשובה החדשה. (6 נק')

שאלה 3 (30 נקודות – 5 נק' כל סעיף)

כפי שנלמד בכיתה, אחת הבעיות העקרוניות של שימוש ב-ECB, היא העובדה שהצפנה של הודעה המורכבת משני בלוקים זהים (כלומר $M=M_1M_2$, כך ש- $M_1=M_2$) יוצרת הודעה מוצפנת המורכבת אף היא משני בלוקים זהים (כלומר $C=C_1C_2$, כך ש- $C_1=C_2$).

לכן, הוצע אופן תפעול חדש בשם ECBC – Electronic Code Book with Counter, כך שההצפנה של הבלוק i היא: $C_i = E_K(M_i \oplus i)$.

- הסבר/י מדוע הצפנה של $M=M_1M_1$ ב-ECBC היא כתב סתר C עבורו שני הבלוקים אינם זהים.
- האם שיוויון בין בלוקים של כתב הסתר מגלה מידע בנוגע לבלוקי ההודעה שלהם? אם כן – תאר/י מהו המידע. אם לא, הסבר/י מדוע.
- הראה/י כי כל התקפת Chosen plaintext על הצופן במוד ECBC, ניתנת להמרה להתקפת Chosen plaintext על הצופן במוד ECB.

המשך השאלה דן באופן התפעול CBC, המצפין את הבלוק ה- i של ההודעה לפי $C_i = E_K(M_i \oplus C_{i-1})$ כאשר $C_0=IV$, עבור ערך IV שנקבע ע"י השולח, ומשורשר לתחילת ההודעה.

- הראה/י כיצד תוקף שמקבל את כתב הסתר המתאים להודעה $M=M_1M_2M_3M_4$ (כלומר את ההודעה המוצפנת $(IV, C_1C_2C_3C_4)$), מסוגל ליצר את כתב הסתר התואם להודעה $M=M_1M_2M_3$, גם ללא ידיעת המפתח.
- הראה/י כיצד תוקף שמקבל את כתב הסתר המתאים להודעה $M=M_1M_2M_3M_4$ (כלומר את ההודעה המוצפנת $(IV, C_1C_2C_3C_4)$), מסוגל ליצר את כתב הסתר התואם להודעה $M=M_2M_3M_4$, גם ללא ידיעת המפתח.
- ניח כי במהלך הצפנת ההודעה $M=M_1M_2M_3M_4M_5$, התקבל כתב הסתר $(IV, C_1C_2C_3C_4C_5)$ כך ש- $C_2=C_4$. הראה/י כיצד תוקף יכול ליצר את כתב הסתר התואם להודעה $M=M_1M_2M_3M_4M_3M_4M_5$, גם ללא ידיעת המפתח.