ד"ר בני פנקס

מבוא לקריפטוגרפיה - מועד א'

החוג למדעי המחשב – אוניברסיטת חיפה
סמסטר א' תשס"ז
7.2.2007

הנחיות:

1. בטופס הבחינה שלושה דפים מלבד דף זה. ודאו כי כולם נמצאים בידכם.
2. בבחינה 5 שאלות שמשקלן שווה. **יש לענות על 4 שאלות בלבד.** (לא יבדקו יותר מ-4 שאלות.)
3. הבחינה עם חומר פתוח.
4. משך הבחינה 2.5 שעות.
5. הנכם רשאים להסתמך על סעיפים קודמים, גם אם לא השבתם עליהם.
6. **נמקו את כל תשובותיכם (פרט לפתרונות סעיפי שאלה 1).** פתרון לשאלות 2-5 ללא הוכחה לא יתקבל.

בהצלחה!

1. ענו על **כל** השאלות הבאות. אין צורך לנמק את התשובות לשאלה זו.

א. מדוע מומלץ להשתמש במערכת אל-גמל במפתח פומבי שהוא ארוך בהרבה מהמפתח של מערכת סימטרית כגון AES ?

ב. אליס ובוב מבצעים הסכמה על מפתח בשיטת Diffie-Hellman בחבורה Z^*_{53}, עם היוצר g=3. אליס שולחת לבוב את המספר 52 (כלומר $g^a=52$), ובוב מחזיר את המספר 27. מהו המפתח עליו הסכימו אליס ובוב?

ג. ברשות אליס ובוב מפתח K הידוע רק לשניהם. אליס בוחרת מפתח פרטי Psig ומפתח פומבי Pver למערכת החתימה של RSA. היא שולחת לבוב הודעה יחידה M ללא הצפנה, ובנוסף שולחת את Pver, חתימה על ההודעה עם המפתח הפרטי של מערכת ה-RSA, וכמו כן MAC המחושב באמצעות K על מפתח וידוא החתימה (כלומר, שולחת את הערכים Pver, RSA-$SIGNATURE_{Psig}(M)$, $MAC_K(Pver)$). שימו לב שאין PKI המאפשר לוודא איזה מפתח פומבי שייך לכל שחקן. איזו מהאפשרויות הבאות נכונה?

1. בוב אינו יכול לוודא לעצמו, וגם אינו יכול להוכיח לאנשים אחרים, שההודעה נשלחה על ידי אליס.
2. בוב יכול לוודא לעצמו שההודעה נשלחה על ידי אליס, אך אינו יכול להוכיח זאת לאנשים אחרים.
3. בוב יכול להוכיח לאנשים אחרים שההודעה נשלחה על ידי אליס, אך אינו יכול לוודא זאת לעצמו.
4. בוב יכול לוודא לעצמו, וגם יכול להוכיח לאנשים אחרים, שההודעה נשלחה על ידי אליס.

ד. סדרו את זמני הריצה של הפעולות הבאות מהקצר לארוך. אם זמן הריצה של פעולה אחת גדול במקצת מזה של אחרת, השתמשו בסימון ">". אם הפרש זמני הריצה משמעותי (בסגר גודל או יותר) השתמשו בסימון ">>". כל הפעולות מתבצעות מודולו אותו מספר N=pq בן 1024 סיביות.

a. הצפנת RSA עם מפתח פומבי $2^{16}+1$.
b. פענוח RSA עם מפתח פומבי $2^{16}+1$.
c. הצפנה במערכת ההצפנה של רבין.
d. פענוח במערכת ההצפנה של רבין.

2. אליס ובוב משתמשים ב-block cipher. לאליס מפתח K1 ולבוב מפתח K2 (אורך כל מפתח 128 סיביות). נסמן ב- E את פעולת ההצפנה. ברצונם להצפין הודעות שאורכן 256 סיביות, אך ידוע שבכל הודעה רק 80 הסיביות הראשונות מכילות מידע ושאר הסיביות תמיד שוות לאפס. המטרה היא שרק מי שברשותו שני המפתחות יוכל לפענח הודעות מוצפנות. אליס ובוב שוקלים את האפשרויות הבאות להצפנת ההודעות:

1. שליחת $E_{K1\oplus K2}(M)$
2. שליחת $E_{K2}(E_{K1}(M))$
3. שליחת $E_{K1}(R), E_{K2}(R\oplus M)$, כאשר R היא מחרוזת אקראית באורך M.

אליס ובוב מניחים שתוקף ישיג הודעה אחת M ואת ההצפנה שלה C, וכן הודעה מוצפנת נוספת C' שברצותו לפענח. הם מקווים שהתקפה כזו (מציאת M' שהוצפן ב-C') תדרוש מהתוקף עבודה של 2^{256} לפחות.

א. הראו שעבור כל אחת מהשיטות המוצעות כאן תוקף יכול למצוא את M' בזמן של בערך 2^{128}. (רמז: Meet in the Middle) (18 נקודות)
ב. איזו מהשיטות הכי קשה לשבירה? (3 נקודות)
ג. איזו מהשיטות הכי קלה לשבירה? (2 נקודות)
ד. איזו מהשיטות הכי יעילה למימוש? (2 נקודות)

3. במערכת RSA המפתח הפומבי של אליס הוא (N,e_1), והמפתח הפומבי של בוב הוא (N,e_2), כאשר e_1 ו-e_2 זרים זה לזה. אותה הודעה M הוצפנה בנפרד על ידי המפתחות הפומביים של אליס ושל בוב, והתקבלו הודעות מוצפנות C_1 ו-C_2, בהתאמה. תוקף אשר יודע את שני המפתחות הפומביים מאזין לשתי הודעות מוצפנות אלו.

א. הראו כיצד התוקף יכול לחשב מספרים שלמים r,s כך שיתקיים $re_1+se_2=1$. (5 נקודות)

ב. התוקף מחשב את $(C_2)^s\cdot(C_1)^r \bmod N$, כיצד מידע זה עוזר לו למצוא את M ? (10 נקודות)

ג. מכיוון ש- $e_1, e_2 >0$, אחד מהערכים r ו-s חייב להיות שלילי. נניח שזהו s. כיצד ניתן לחשב את $(C_2)^s$ במקרה זה? (10 נקודות)

4. שאלה זו דנה במערכת להסכמה על מפתח לשיחת ועידה.
שחקנים $A_1,A_2,\ldots,A_n,B$ רוצים להסכים על מפתח משותף שיהיה ידוע להם אך ישמר בסוד מפני כל מאזין. הם משתמשים במערכת הבאה:

- יהא p ראשוני ויהא g איבר מסדר q ב-Z_p^*, כאשר q הוא ראשוני גדול.
- המשתמש B בוחר באקראי מספר b ב-$\{1,\ldots,q\}$ ומחשב את $y=g^b \bmod p$.
- כל שחקן אחר A_i בוחר באקראי מספר a_i ב-$\{1,\ldots,q\}$ ומחשב את $x_i=g^{a_i} \bmod p$.
- השחקן A_i שולח את x_i ל-B ומקבל בחזרה את $z_i=(x_i)^b \bmod p$.

א. (5%) הראו כי בהינתן z_i ו-a_i, השחקן A_i יכול לחשב את y.

ב. (13%) הסבירו מדוע y יכול לשמש כמפתח שיחת הועידה. כלומר, הסבירו מדוע בסוף הפרוטוקול $A_1,\ldots,A_2,B$ יכולים לחשב את y, ומדוע (בצורה לא פורמלית) מאזין אינו יכול לחשב את y.

ג. (7%) הוכיחו את הטענה הקודמת. כלומר, הראו שאם ישנו אלגוריתם יעיל E, שבהינתן הערכים הפומביים שנשלחים בפרוטוקול יכול לחשב את y, אזי ישנו אלגוריתם D שיכול לשבור את בעיית דיפי-הלמן החישובית (computational Diffie-Hellman problem). האלגוריתם D מקבל כקלט g^a ו-g^b מודולו p ואמור לחשב את g^{ab}. הוא יכול להשתמש באלגוריתם E כקופסא שחורה. ניתן להוכיח רק למיקרה של שני שחקנים, A_1 ו-B. (רמז: בהינתן קלטים g,g^b האלגוריתם E יחשב את $g^{1/b}$. ניתן להשתמש בכך בשלב ראשון של הרדוקציה.)

5. נדון בשיטה הבאה לבנות פונקצית Hash ממערכת הצפנה: הניחו שמערכת ההצפנה משתמשת במפתח באורך L להצפין הודעות באורך L. נתונה הודעה $M=m1,m2,\ldots,mn$ המכילה n בלוקים, כאשר כל בלוק mi הוא באורך L. ה- Hash מחושב בתהליך הבא: $h1=m1$, $h2=E_{m2}(h1)$, $h3=E_{m3}(h2)$, וכן הלאה. פלט פונקצית ה-Hash הוא h_n. הקלט לפונקציה הוא תמיד באורך של לפחות שני בלוקים ($n>1$).

א. האם ניתן למצוא בצורה יעילה התנגשויות בפונקצית ה-Hash כאשר E היא one-time-pad ? (8 נקודות)

ב. האם ניתן למצוא בצורה יעילה התנגשויות בפונקצית ה-Hash כאשר E היא AES ? (9 נקודות)

ג. משתמש אחר הציע פונקצית Hash שונה אך דומה: ה- Hash מחושב בתהליך הבא: $h1=m1$, $h2=E_{h1}(m2)$, $h3=E_{h2}(m3)$, וכן הלאה. פלט פונקצית ה-Hash הוא h_n. האם ניתן למצוא בצורה יעילה התנגשויות בפונקציה זו כאשר E היא one-time-pad וכאשר היא AES ? (8 נקודות)