ד"ר בני פנקס

מבוא לקריפטוגרפיה - מועד ב'

סמסטר א' תש"ע
1.3.10

הנחיות:

1. בטופס הבחינה שני דפים מלבד דף זה. ודאו כי כולם נמצאים בידכם.
2. **בבחינה 4 שאלות שמשקלן הכולל הוא 110 נקודות. הציון הסופי יהיה סכום הנקודות שיצטברו בכל השאלות, אך לא יותר מ-100.**
3. **סטודנט אשר לא יענה על סעיף מסוים ויכתוב בברור במחברת הבחינה "*לא עניתי על סעיף X*" יקבל 20% מהנקודות של הסעיף.**
4. הבחינה עם חומר פתוח.
5. משך הבחינה שלוש שעות. לא תינתן הארכה.
6. הנכם רשאים להסתמך על סעיפים קודמים, גם אם לא השבתם עליהם.
7. **נמקו את כל תשובותיכם, פרט לפתרונות סעיפי שאלה 1. פתרון לשאלות 2-4 ללא הוכחה לא יתקבל.**

בהצלחה!

1. (20%) ענו על **כל** הסעיפים הבאים שלכולם משקל שווה. אין צורך לנמק את התשובות לשאלה זו.

א. רק אחת מהטענות הבאות נכונה. העתיקו אותה לטופס התשובות.
1) חישוב MAC של הודעה יעיל יותר מחישוב חתימה על אותה הודעה (בשיטות שנלמדו בהרצאה).
2) בפרוטוקול SSL מחושבת חתימה על כל הודעה שנשלחת על ידי כל אחד מהצדדים בתהליך החלפת המפתחות.
3) בהינתן MAC של הודעה שחושב על ידי אליס, בוב יכול להוכיח לכל אחד אחר שההודעה נשלחה על ידי אליס.
4) שימוש ב-MAC לאימות הודעות אינו דורש מהצדדים להסכים מראש על מפתח משותף.

ב. (5%) תארו בקצרה (בשלוש שורות לכל היותר) את ההבדלים העיקריים בין פונקצית אותנטיקציה (MAC) ובין פונקצית תמצות (HASH).

ג. (5%) הסבירו בקצרה (עד שלוש שורות) מה ההבדל העיקרי בין בטיחות מושלמת ובטיחות חישובית (computational security).

ד. מדוע משתמשים ב-IV קבוע ב-MAC-CBC ?

4. (30%) נדון בשיטה הבאה לבנות פונקצית Hash ממערכת הצפנה: הניחו שמערכת ההצפנה משתמשת במפתח באורך L להצפין הודעות באורך L. נתונה הודעה M=m1,m2,…,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. (10%) האם ניתן למצוא בצורה יעילה התנגשויות בפונקצית ה-Hash כאשר E היא one-time-pad ?

ב. (10%) האם ניתן למצוא בצורה יעילה התנגשויות בפונקצית ה-Hash כאשר E היא AES ?

ג. (10%) 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 ?

2. (30%) (מערכת מבוזרת לפענוח הצפנת אל-גמל.) יהא p ראשוני, ויהא g גנרטור של Z_p^*. המספר xהוא מפתח פרטי של מערכת ההצפנה של אל גמל.
א. (3%) ראשית, הסבירו כיצד פועלת מערכת ההצפנה של אל-גמל.
ב. (11%) בכדי להגן על המפתח הפרטי הוא מחולק למספר חלקים המאוחסנים בשרתים שונים. הניחו שנבחרים שלושה מספרים אקראיים x1,x2,x3 בתחום

[1,p-1], תחת האילוץ x1+x2+x3=x mod p. ישנם שלושה שרתים. השרת הראשון שומר את x1, השרת השני שומר את x2, והשלישי את x3. כאשר אליס רוצה לפענח הצפנה C, היא מבצעת את הפעולות הבאות: (1) שולחת את C לכל אחד מהשרתים. (2) שרת i מבצע חישוב בעזרת הערך xi הידוע לו, ושולח את התוצאה Mi לאליס. (3) אליס משתמשת בערכים M1,M2,M3 לחישוב הפענוח של C.
הסבירו כיצד כל שרת מחשב את Mi, וכיצד אליס מחשבת את פענוח ההודעה.

ג. (6%) אם יריב פורץ לשרת הראשון ולומד את x1, האם הוא יכול לפענח הודעות מוצפנות? אם הוא פורץ לשרת הראשון ולשרת השני ולומד את x1 ואת x2, האם אז הוא יכול לפענח הודעות מוצפנות? מדוע?

ד. (10%) הסבירו כיצד לשנות את תכנון המערכת בכדי לספק עמידות בפני נפילות: המערכת החדשה תמשיך לעבוד גם אם שרת אחד יפסיק לעבוד. אליס תוכל לפנות אל שני השרתים האחרים, לשלוח להם את C ולקבל מידע שיאפשר לה לפענח את C. יתקיימו התכונות הבאות: (1) יריב שפורץ לשרת בודד לא יוכל לפענח הודעות. (2) יתכן ושרת יאחסן יותר ממפתח יחיד. (3) לא מתבצעת כל תקשורת בין השרתים. רמז: ניתן להשתמש ברעיונות משיטת שיתוף הסודות של Shamir.

3. (30%) שאלה זו עוסקת בשיטות לחלוקת סוד (secret sharing). ישנם $n=n_1n_2$ משתתפים, המחולקים ל-n_1 קבוצות <u>זרות</u> של n_2 משתתפים בכל אחת. נתונים ספים (thresholds) כדלקמן: $t_1 <= n_1$, ו- $t_2 <= n_2$. קבוצה S של משתתפים שייכת למבנה הגישה אם ישנן לפחות t_1 קבוצות כך ש-S מכילה לפחות t_2 משתתפים מכל אחת מהן. קבוצת משתתפים רשאית לקבל את הסוד אם, ורק אם, היא שייכת למבנה הגישה.

א. (6%) הראו כי מבנה גישה זה הוא מיקרה כללי של t-out-of-n secret sharing שנלמד בכיתה (כלומר, הראו שניתן לממש t-out-of-n secret sharing באמצעות מבנה גישה זה).

ב. (6%) האם יתכנן מצב בו ישנן שתי קבוצות, S1 ששייכת למבנה הגישה, ו-S2 שאינה שייכת למבנה הגישה, כך שב-S2 ישנם יותר משתתפים ב-S1 ?

ג.(6%) תארו עבור מבנה הגישה הזה שיטה לחלוקת סוד המבוססת על שיטת חלוקת הסוד של שמיר, כאשר הסוד והחלקים לקוחים מתוך Z_p עבור p>n.

ד. (6%) הוכיחו כי כל קבוצה S השייכת למבנה הגישה יכולה לשחזר את הסוד בשיטה שבניתם בסעיף ב'.

ה. (6%) תהא T קבוצת משתתפים שאינה שייכת למבנה הגישה. הראו כי לכל קביעה של חלקי סוד לשחקנים ב-T, כל סוד s ב- Z_p הוא אפשרי. כלומר, קיימת חלוקה של הסוד s בה אלו הם החלקים הניתנים לשחקנים ב-T. (לשם פישוט ההוכחה ניתן להוכיח רק למקרה בו הקבוצה T מתקבלת מהורדת שחקן אחד מקבוצה מבנה הגישה.)