הטכניון - מכון טכנולוגי לישראל
הפקולטה למדעי המחשב

מבחן בקריפטולוגיה מודרנית - 236506

סמסטר חורף, תשס"ד
מועד ב', 18.3.2004

מרצה: אלי ביהם
מתרגל: אלעד ברקן

משך המבחן: שלוש שעות.

במבחן 4 שאלות. ענה על כולן.

מותר להשתמש בכל חומר עזר לא אלקטרוני (בפרט אסור טלפון סלולרי!)

הקדש את 10 הדקות הראשונות לקריאת כל השאלות והבנתן.

ענה תשובות קצרות וברורות ככל האפשר. נמק את כל תשובותיך.

הקצה מראש שני עמודים במחברתך לכל שאלה לפי סדר השאלות.

כתוב בצורה מסודרת ונקיה ובכתב ברור. תשובות לא ברורות לא תיבדקנה.

בהצלחה!

© כל הזכויות שמורות.

<u>שאלה 1</u> (20 נקודות)

בתרגול ראינו אלגוריתם להוצאת שורש מודולו p, עבור $p=4k+1$. לצורך האלגוריתם נדרשנו לחשב gcd של פולינומים מצורה מסויימת, בפרט: $\gcd(x^{(p-1)/2}-1,\ x^2+ax+b)$.
בשאלה זו נעסוק בישימות חישוב gcd כנ"ל.

באופן כללי gcd של פולינומים ניתן לחישוב באופן דומה לחישוב כפי שנלמד בכיתה עבור שלמים, תוך שימוש בחלוקת פולינומים. ה-gcd יחיד עד כדי מכפלה בפולינום האפס (מכפלה בקבוע מ Z^*_p). מקדמי הפולינום הם איברים ב-Z_p. שימו לב שאלגוריתם ה-gcd מבצע חילוק אך ורק על מנת לקבל את השארית.

א. בצע חילוק ארוך של הפולינום x^4-x^3+x+1 פי $x+2$. מהו פולינום המנה, ומהו פולינום השארית?
ב. הראה שניתן לחשב gcd עבור פולינומים מהצורה הנ"ל $(x^{(p-1)/2}-1,\ x^2+ax+b)$ תוך שימוש בלכל היותר שלוש חלוקות פולינומים.
ג. הראה שמספר הצעדים באלגוריתמי החילוק בסעיף ב' עשוי להיות סדר גודל של p, דהיינו אקספוננציאלי ב- $\log p$. הסק ששיטה חלוקה זו אינה יעילה במקרה שלנו.
ד. הצע דרך יעילה לחשב את ה-gcd הנ"ל. מה סיבוכיותה?
הדרכה: כיצד היית מחשב ביעילות את $3^{(p-1)/2} \bmod q$ (עבור $p\neq q$)?

© כל הזכויות שמורות.

שאלה 2 (20 נקודות)

בהרצאה הוצגה שיטת רבין בצורה שונה במקצת מצורתה במאמר המקורי.
רבין הגדיר את השיטה ע"י בחירת n כמו ב-RSA וערך b אקראי, והמפתח הפומבי הינו (b,n). רבין הציע להצפין הודעה M ע"י ביצוע:

$$C=M(M+b) \bmod n$$

בהרצאה הצגנו את המקרה עם b=0.

א. תאר כיצד ניתן לפענח (התעלם מבעיית ריבוי השורשים).

ב. הוכח שקיום אלגוריתם לפתרון משוואות מהצורה $C\equiv M(M+b) \bmod n$, כאשר b,C נתונים, מאפשר פירוק של n.

ג. נתונה חתימה S על הודעה M בשיטה של רבין שתיארנו בכיתה (ללא תוספת אקראיות כפי שמופיע בשקף 326 בגירסה האחרונה של השקפים), אך לבודק יש חומרה שיודעת לבדוק רק בשיטה המקורית של רבין שתוארה לעיל, וכן בשל תקלת חומרה היא עובדת רק כאשר $b\neq 0$ mod n. הראה כיצד ניתן להשתמש בחומרה הנ"ל לבדיקת חתימה בשיטה שתארנו בכיתה.

© כל הזכויות שמורות.

שאלה 3 (30 נקודות)

שאלה זו עוסקת בשיתוף סוד. בתרגיל הבית התמודדנו עם הבעיה שיתכן ששחקנים חושפים שתפים(Shares) שיקריים, וכך מונעים איחזור הסוד. בשאלה זו נעסוק בבעיה שמחלק הסוד (להלן ה"דילר") עשוי לחלק אותו בצורה לא קונסיסטנטית: בחלוקת הסוד של שמיר, הדילר מחלק שתפים ל-n השחקנים. השתפים מהווים n נקודות על פולינום מסדר k-1. אך, דילר רמאי עשוי לחלק שתפים שאינם נקודות בפולינום מסדר k-1. (אלא סדר גדול יותר). הנזק שהדילר גורם בכך, הוא שקבוצות שונות של k שחקנים, יאחזרו סודות שונים, ולא את אותו הסוד.

יהי $q>n>2$ ראשוני, ו-p ראשוני כך ש $q|p-1$. יהי g יוצר ב- Z^*_p, ו-G_q כל האיברים ב-Z^*_p מסדר q, בתוספת האיבר 1 (יש q איברים ב-G_q, המהווה תת-חבורה ציקלית של Z^*_p, במילים אחרות G_q היא כל האיברים a עבורם $a^q\equiv 1 \pmod p$). שים לב שכל האיברים ב- G_q פרט ל-1 הינם יוצרים ב-G_q. יהי h יוצר ב-G_q .

q, p, h, g – פרמטרים פומביים.

הסכמה: לדילר סוד $S\in Z_q$, הדילר בוחר באופן רנדומי $a_1,\ldots,a_{k-1} \in Z_q$. ומחשב את הפולינום:

$$C(x)=S+a_1x+a_2x^2+\cdots+a_{k-1}x^{k-1} \pmod q$$

הדילר מחלק את $Si=C(i)$ לשחקן ה-i, כאשר $i\in\{1,\ldots,n\}$.

שימו לב: g יוצר של Z^*_p, אך לא נשתמש בו בשאלה, h איבר מסדר q ב-Z^*_p.

א. הסבר בקצרה כיצד קבוצה של k שחקנים המשתפת פעולה יכולה למצוא את הסוד, בעוד קבוצה של k-1 שחקנים לא לומדת דבר מתוך השתפים.

כעת, בנוסף, הדילר מפרסם התחייבויות לשתפים, ע"י פרסום $h^{Si} \bmod p$.

ב. הסבר כיצד בודק שחקן שהשתף שהוא קיבל תואם את הפרסום.

ג. שחקן חיצוני, שאין בידו אף שתף, אך יש לו גישה לכל המידע הציבורי והמידע שהדילר פרסם רוצה לבדוק שהדילר הוגן (כלומר שכל קבוצה של k שחקנים תאחזר את אותו הסוד). הסבר כיצד השחקן החיצוני יוכל לבצע בדיקה זו (רמז: האם תוכל לחשב את $h^S \pmod p$).

ד. האם בהנתן כל המידע שמחלק ומפרסם הדילר, הסכמה עדיין נשארה Secret Sharing (כלומר האם כל קבוצה של k-1 שחקנים לא לומדת דבר על הסוד מבחינת תורת האינפורמציה)?

ה. האם איברי G_q הם כולם QR ב-Z^*_p, או כולם QNR ב-Z^*_p, או חלק מהאיברים הם QR וחלק QNR ב-Z^*_p, ציין יש כמה מכל סוג אם תוכל?

ו. בהנתן איבר שהוא QR ב-G_q, הראה שאחד משורשיו ב-G_q והשני לא.

ז. שחקן חיצוני שיצר קשר עם חוצנים (חיזרים), קיבל לידיו מכונה פלאית, שבהנתן $h^x \bmod p$, $0\le x<q$, מחזירה את הביט התחתון של x. האם בעזרת מכונה פלאית זו יוכל השחקן בקלות למצוא את כל S? ביטים אחדים מ-S? ביט אחד מ-S? אף ביט על S?

© כל הזכויות שמורות.

שאלה 4 (30 נקודות)

לפני שנים רבות בארץ זולו הוצעה שיטת החתימה החד פעמית הבאה:

- החותם בוחר 40 מפתחות DES Ki באקראי, ומפרסם בקובץ ציבורי המאוחסן אצל צד שלישי בטוח את $DES_{Ki}(0)$.
- לביצוע החתימה על מסמך m, החותם מצפין את m ב-DES תחת 40 המפתחות ושולח את ההצפנות למקבל (ולעולם לא חותם שנית בעזרת 40 המפתחות הללו).
- המקבל בוחר באקראי 20 הודעות מוצפנות ושולח לחותם את האינדקסים שלהם.
- החותם שולח למקבל את 20 המפתחות המתאימים.
- המקבל מפענח את 20 ההודעות ומוודא שתוכנן הוא m, ומפענח את 20 ההצפנות בקובץ הציבורי ומוודא שמתקבל 0 – אם זה לא המצב: עוצר ומכריז על החותם כרמאי.

א. מה הסיכוי שלאחר ביצוע מוצלח אחד של פרוטוקול החתימה, בין 20 ההודעות שלא פוענחו יש הצפנה מזוייפת (כלומר ההודעה לא נוצרה ע"י $E_{Ki}(m)$, כאשר $E_{Ki}(0)$ מופיע בקובץ הציבורי)? (למשל החותם הצליח להצפין הודעה שונה מ-m, או הצפין בעזרת מפתח אחר – ולא נתפס ע"י המקבל)

ב. מה הסיכוי שלאחר ביצוע מוצלח אחד של פרוטוקול החתימה, בין 20 ההודעות שלא פוענחו אין אף הצפנה של m ע"י מפתח מהקובץ הציבורי (כלומר אין אף הצפנה בעזרת מפתח Ki שעבורו בקובץ הציבורי יש $DES_{Ki}(0)$) ?

ג. כמה הפעלות DES נדרשות לזייפן לייצור הצפנה בודדת של m תחת אחד מ-40 המפתחות של מישהו אחר (בהם טרם השתמשו לחתימה)? ועבור יצירת 20 הצפנות תחת 20 מפתחות מה-40?

ד. במקרה שהחותם מנסה להתכחש לחתימה, הולכים החותם והמקבל לשופט. המקבל מגלה את 40 ההודעות המוצפנות, ואת ההודעה m ואז החותם מגלה לשופט את 40 המפתחות.
על השופט להחליט האם החותם אכן חתם למקבל על המסמך m, או האם לא חתם.
תן קריטריון שבעזרתו יוכל השופט לפסוק נכון. נסה לתת את הקריטריון שיביא למינימום את מספר הפסיקות השגויות של השופט.

ה. האם מספיק שהמקבל יגלה לשופט רק את 20 ההודעות שנשארו מוצפנות ואת m, במקום את כל ה-40?

ו. ידוע ששקיפות ציבורית מהווה ערך עליון בארץ זולו, ובשל כך כל המידע שנאמר במשפט מפורסם בגלוי. מה יעשה שופט כאשר יבוא אליו אדם עם חתימה שנוצרה ע"י וקטור בקובץ הפומבי ששימש כבר לבדיקת חתימה ע"י שופט בעבר?

ז. הראה כיצד חותם שאינו רוצה לקיים התחייבותו פונה לידיד אחר ומשתף איתו פעולה כדי לבטל חתימה שנוצרה בעבר.

ח. איך תתקן את הבעיה מהסעיף הקודם? תן הצעה פשוטה וקלה ליישום (עם שינוי מינימלי לשיטה).

© כל הזכויות שמורות.