הטכניון - מכון טכנולוגי לישראל
הפקולטה למדעי המחשב

מבחן בקריפטולוגיה מודרנית - 236506

סמסטר חורף, תשס"ג
מועד ב', 13.3.2003

מרצה: אלי ביהם
מתרגל: אור דונקלמן

משך המבחן: שלוש שעות.

במבחן 4 שאלות. ענה על כולן.

מותר להשתמש בכל חומר עזר לא אלקטרוני.

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!

שאלה 1

סיבוכיות הזמן של האלגוריתם הטוב ביותר לפירוק נכון להיום (Number Field Sieve) היא $e^{O((\log n)^{\frac{1}{3}}(\log\log n)^{\frac{2}{3}})}$, ואינה תלויה בגודל הגורם הקטן ביותר של n, אלא בגודל המספר הפריק n עצמו.
לפיכך, שיטת החתימה של רבין בטוחה כנגד זיוף (בהנחה שהתקפות Chosen ciphertexts אסורות), גם אם משנים את מספר הגורמים של n ללא שינוי בסדר הגודל שלו.
פרופ' ניבר, הציע שיטת חתימה חדשה המבוססת על שיטת רבין, והמנצלת את האבחנה הנ"ל. במקום להשתמש ב-$n=pq$, המשתמש מפרסם $n = p^2q$. וכדי לחתום על הודעה m המשתמש מחשב שורשי ההודעה m מודולו n, ואחד השורשים הוא החתימה.

א. סעיף זה עוסק במספר השורשים השונים של m מודולו מספר פריק מהצורה הנ"ל.
נתון $s = p^e$ כאשר p ראשוני המקיים $p \neq 2$ ו- $e \in N$. הראה כי למשוואה $x^2 = c \bmod s$ לכל היותר שני שורשים בדיוק לכל $c \in QR(s)$.

ב. הראה כי עבור $s = 2^e$ לכל e המקיים $e > 2$, הטענה הנ"ל לא נכונה.

ג. בסעיף זה נתחיל בפיתוח שיטה לחישוב השורש של מספר מודולו p^2.
הראה כיצד בהנתן x כך ש- $x^2 \equiv c(\bmod p)$ (ו-$p>c$), ניתן למצוא x', כך שמתקיים: $x'^2 \equiv c(\bmod p^2)$. מהי סיבוכיות השיטה שמצאת?

ד. בסעיף הקודם ראינו שיטה שמטפלת בהודעות m אשר ערכן מודולו p ומודולו p^2 זהה. מכיוון שזהו חלק קטן בלבד ממרחב ההודעות, הראה כיצד בהנתן x כך ש- $x^2 \equiv c(\bmod p)$, ניתן למצוא x', כך שמתקיים: $x'^2 \equiv c'(\bmod p^2)$, כאשר $c' \equiv c(\bmod p)$ ו- $c' \neq c(\bmod p^2)$.
מהי סיבוכיות השיטה שמצאת?

ה. על סמך סעיפים ג' ו-ד', האם השיטה החדשה יעילה יותר ביחס לשיטת רבין (עבור אותו אורך מפתח פומבי)?

שאלה 2

א. הראה כי עבור צופן לינארי קריפטאנליזה דיפרנציאלית לא יכולה לעבוד.
תזכורת: צופן לינארי הינו צופן המקבל כתב סתר P באורך n ביטים. הצופן מתייחס לכתב הסתר כוקטור בינארי באורך n, ומחשב את כתב הסתר תחת מפתח k לפי הנוסחא $E_k(P) = M \cdot P + b$. כאשר אם כתב הסתר C הינו באורך m ביטים ($m \geq n$), אזי M הינה מטריצה של $m \times n$ ביטים ו-b וקטור בינארי באורך m ביטים (M ו-b יכולים להיות תלויים ב-k). שימו לב כי פעולות החיבור והכפל של הביטים הן XOR ו-AND בהתאמה.

ב. כדי לשפר את העמידות של DES כנגד התקפות דיפרנציאליות הוצע לבצע לקלט XOR עם תת מפתח בן 64-ביט שנגזר מהמפתח המקורי. נסמן את DES ששונה ב- DESY. כלומר, אלגוריתם ייצור תתי-המפתחות החדש מייצר בנוסף ל-16 תתי מפתחות של 48-ביט כל אחד, גם תת-מפתח K_{17}, באורך של 64-ביט, ומתקיים: $DESY_K(P) = DES_K(P \oplus K_{17})$.
האם צופן זה חזק יותר כנגד קריפטאנילזה דיפרנציאלית?

ג. כדי לשפר את בטיחות DESY הוצע ליצר עוד תת מפתח בן 64-ביט, ולבצע XOR של כתב הסתר של DESY עימו. כלומר, אלגוריתם ייצור המפתחות החדש מייצר גם את K_{18}, וההצפנה בגרסא החדשה של DES הקרויה DESX היא: $DESX_K(P) = DES_K(P \oplus K_{17}) \oplus K_{18}$.
האם צופן זה חזק יותר כנגד קריפטאנליזה דיפרנציאלית?

שאלה 3

במועד א', שאלה 4, ראינו כי אם מעוניינים לחתום חתימת RSA במפתח פומבי נתון *(n,e)* על ההודעה להיות במבנה מסוים, אחרת, ניתן לזייף הודעה וחתימה עליה ע"י בחירת *sig* באופן אקראי וחישוב ההודעה $m = sig^e \bmod n$. הצמד *(m,sig)* הינו הודעה וחתימה חוקי.

כדי לפתור את הבעיה שתוקף יכול לייצר צמד הודעה-חתימה חוקי, יצא מכון התקנים האירו-אסיאוקייני בבקשה לפתרון הבעיה תוך שימוש ב-RSA כפונקציית החתימה עצמה (כלומר הפעולה שרק החותם יודע לבצע הינה פענוח RSA).

עבור כל הצעה מהבאות קבע האם צמד הודעה-חתימה חוקי ניתן ליצירה רק ע"י בעל המפתח הפרטי. אם כן – הוכח. אחרת – הראה כיצד משתמש שאינו בעל המפתח הפרטי מייצר צמד הודעה-חתימה חוקי.
הבחן בין המקרים בהם הזייפן יכול לייצר מספר רב מאוד של הודעות, לבין מספר מצומצם של הודעות, וכן האם פעולת הזיוף דורשת חתימות קודמות או לא.

א. הצעת פרוייקט האיחוד האירופאי: בהנתן הודעה *m* החותם מחשב *h(m)* כאשר *h()* הינה פונקציית תמצות בטוחה. החתימה היא $sig(m) = h(m)^d \bmod n$.

ב. הצעת פרוייקט האיחוד האסייתי: בהנתן הודעה *m* כך ש- $|m| < \left\lfloor \frac{|n|}{2} \right\rfloor$ צמד ההודעה-חתימה הוא $sig(m) = (m \| m)^d \bmod n$ כאשר $\|$ היא פעולת השרשור של מחרוזות.

ג. הצעת הפרוייקט התת-קרקעי הראשון: בהנתן הודעה *m* צמד ההודעה-חתימה הוא $sig(m) = (2m)^d \bmod n$.

ועדת האיחוד האירופאי בחרה במפתח הפומבי *(n,3)* והחליטה כי מכיוון שחישוב *h()* דורש הרבה זמן היא משתמשת ב- $sig(m) = (m \| c)^d \bmod n$ כאשר *c* הינה מחרוזת באורך 32 ביט של אפסים. מיד לאחר שפירסמה את השיטה החדשה והמפתח, טען המומחה האוקיאני הנודע אוסטרל זילנד כי ביכולתו לזייף צמדי הודעות-חתימות לגיטימי עבור השיטה החדשה של הוועדה.

ד. הראה כיצד מבצע אוסטרל זילנד את פעולת הזיוף. חשב את סיבוכיות ההתקפה שלו.

ה. הראה כי גם אם הועדה תבחר קבוע אחר, ניתן יהיה לזייף צמדי הודעה-חתימה חוקיים. מה סיבוכיות ההתקפה כעת?

שאלה 4

שאלה זו עוסקת בהוכחת זהות. לפני תחילת ההזדהות בוחר המוכיח באקראי מספר ראשוני גדול p ואיבר $\alpha \in Z_p^*$. המוכיח בוחר באקראי $1<m<p-1$ מחשב $\beta = \alpha^m \bmod p$ ומפרסם את (p,α,β) כוקטור הפומבי שלו לצורך הזדהות.

כאשר המוכיח **P** מעוניין להוכיח למוודא **V** שהוא יודע את m (כלומר את הזהות שלו), הם מבצעים את הפרוטוקול הבא $t=60$ איטרציות:

1. **P** בוחר באקראי $1<i<p-1$ ושולח למוודא את $\gamma \equiv \alpha^i \bmod p$.
2. **V** בוחר באקראי $j \in \{0,1\}$ ושולח את j ל-**P**.
3. **P** מחזיר את $k = i + jm$ למוודא **V**.
4. המוודא בודק ש- $\alpha^k \equiv \gamma\beta^j \pmod p$.

א. הראו כי הפרוטוקול הנ"ל הינו פרוטוקול אפס מידע.

כדי לחסוך בזמן הציע פרופ' קוני-למל מאוניברסיטת קהיר, לבצע את ההוכחה באופן הבא:

1. **P** בוחר באקראי t ערכים $1 < i_r < p-1$ ושולח למוודא את אוסף ה- $\gamma_r \equiv \alpha^{i_r} \bmod p$.
2. **V** בוחר באקראי t ערכים $j_r \in \{0,1\}$ ושולח אותם ל-**P**.
3. **P** מחזיר את אוסף ערכי ה- $k_r = i_r + j_r m$ ל-**V**.
4. **V** בודק שלכל $1<r<t$ מתקיים $\alpha^{k_r} \equiv \gamma_r \beta^{j_r} \pmod p$

ב. האם תשובתך לסעיף א' עדיין תקפה? מדוע?

נשים לב כי הפרוטוקול החדש והפרוטוקול המקורי הם בעלי אותה סיבוכיות תקשורת, כלומר, אם אנו רוצים להשיג שהסיכוי ש-**P** שאינו יודע את m יצליח לשכנע את **V** להיות קטן מ- 2^{-t}, אותה כמות תקשורת תעבור בין המוכיח והמוודא. לפיכך הציע פרופ' שני לשנות את סעיפים 3 ו-4 של הפרוטוקול ולבצע את ההוכחה באופן הבא:

1. **P** בוחר באקראי t ערכים $1 < i_r < p-1$ ושולח למוודא את אוסף ה- $\gamma_r \equiv \alpha^{i_r} \bmod p$.
2. **V** בוחר באקראי t ערכים $j_r \in \{0,1\}$ ושולח אותם ל-**P**.
3. **P** מחזיר את $k = \sum_{r=1}^{t} i_r + m\sum_{r=1}^{t} j_r \pmod{p-1}$ ל-**V**.
4. **V** בודק שמתקיים $\alpha^k \equiv \prod_{r=1}^{t} \gamma_r \beta^{j_r} \pmod p$.

ג. האם הפרוטוקול החדש הינו פרוטוקול אפס ידע? אם לא, הסבר מדוע. אם כן, הראה סימולטור וציין מה הסיכוי ש-**P** שאינו יודע את m יצליח לרמות?
בסעיף זה אין צורך לבצע את החישובים עצמם. ניתן לתת נוסחא (ולהסביר מדוע זו הנוסחא הנכונה).

ד. הצג שיפור שיצמצם את כמות ההודעות ש-**V** שולח מ-t ל-1. אסור לשיפור לשנות את תשובתך לסעיף ג'.