אוניברסיטת בן-גוריון בנגב
Ben-Gurion University of the Negev
The University celebrates its 30th Anniversary

המחלקה למדעי המחשב

דר' עמוס ביימל

קריפטוגרפיה – מועד ב'

סמסטר ב' תש"ס
5.7.2000

הנחיות:

1. בטופס הבחינה שני עמודים מלבד עמוד זה.ודאו כי כולם נמצאים בידכם.
2. בבחינה 4 שאלות שמשקלן אינו שווה. יש לענות על כולן.
3. הבחינה עם חומר פתוח.
4. נמקו את כל תשובותיכם. פתרון ללא הוכחה לא יתקבל.
5. משך הבחינה 3 שעות.
6. מומלץ לא להיתקע זמן רב מדי על שום סעיף.
7. הנכם רשאים להסתמך על סעיפים קודמים, גם אם לא השבתם עליהם.

בהצלחה!

שאלה 1 [22 נקודות]

תהי $f:\{0,1\}^n \to \{0,1\}^n$ פונקציה חד-כיוונית, שבנוסף היא חד-חד ערכית. נסמן $m = 2n$.

סעיף א [11 נקודות]

נגדיר את הפונקציה $g:\{0,1\}^m \to \{0,1\}^m$ הבאה:
בהינתן קלט x,y נאתחל $y_0 = y$ ו- $x_0 = x$ ועבור $0 \le i$ נחשב
$y_{i+1} = x_i \oplus f(y_i)$ ו- $x_{i+1} = y_i$. הפלט של g על קלט x,y הוא x_{10}, y_{10}. האם g היא פונקציה חד-כיוונית?

סעיף ב [11 נקודות]

נגדיר את הפונקציה $h:\{0,1\}^m \to \{0,1\}^m$ הבאה:
בהינתן קלט x,y נאתחל $y_0 = y$ ו- $x_0 = x$ ועבור $0 \le i$ נחשב
$y_{i+1} = y_i \oplus f(x_i)$ ו- $x_{i+1} = y_i$. הפלט של h על קלט x,y הוא x_2, y_2. האם h היא פונקציה חד-כיוונית?

הנחיות:

בשני הסעיפים יש להוכיח את תשובותיכם.

- כדי להוכיח שפונקציה q היא חד-כיוונית יש להראות כי אם יש אלגוריתם המחשב את q^{-1} אזי יש אלגוריתם המחשב את f^{-1}.
- כדי להוכיח שפונקציה q אינה חד-כיוונית יש להראות אלגוריתם המחשב את q^{-1}.

שאלה 2 [23 נקודות]

נסתכל בסכמת חלוקת הסוד של שמיר כאשר מספר המעבדים הוא n, מספר המעבדים שיכולים לשחזר את הסוד הוא t ותחום הסודות הוא Z_p. בשאלה זו המחלק הוא הוגן אבל יש מעבד אחד רמאי המחליף את החלק שלו באיבר מ- Z_p.
המעבדים שולחים את החלקים שלהם ל"בודק" שרוצה לגלות מיהו הרמאי.
כלומר, לבודק ישנם n זוגות (s_j, j) כאשר s_j הוא החלק שמעבד j מציג כחלק שקיבל מהמחלק.

סעיף א [12 נקודות]

הוכיחו כי אם $n = t+1$ אזי הבודק לא יכול לדעת מיהו המעבד הרמאי.

סעיף ב [11 נקודות]

הניחו כי $n > t+1$. תארו אלגוריתם יעיל המאפשר לבודק למצוא את המעבד הרמאי. יש להוכיח את נכונות האלגוריתם ולהסביר מדוע הוא יעיל.

שאלה 3 [33 נקודות]

יהיו p ו-q ראשוניים גדולים ו-$N = pq$. נבחר e כך ש-$\gcd(e, \varphi(N)) = 1$.

סעיף א [4 נקודות]

הוכיחו כי הפונקציה $f : \mathbb{Z}^*_N \to \mathbb{Z}^*_N$ הבאה $f(C) = C^e \bmod N$ היא פרמוטציה.

סעיף ב [4 נקודות]

הוכיחו כי קיימים שלמים i, j, כאשר $0 < i < j$, כך ש-$e^i \equiv e^j \pmod{\varphi(N)}$.

סעיף ג [10 נקודות]

הוכיחו כי קיים שלם $0 \le k$ כך שלכל $C \in \mathbb{Z}^*_N$ מתקיים $C^{e^k} \equiv C \pmod N$.

סעיף ד [15 נקודות]

נתאר התקפה על RSA כאשר k הנ"ל הוא קטן. כדי לפענח את הקריפטוגרמה $C = \mathrm{RSA}(M, (N, e))$, כאשר ידועים C והמפתח הציבורי בלבד, מתקיף מחשב את הסדרה $C, C^e, C^{e^2}, C^{e^3}, \ldots$ (החישובים הם מודולו N) עד שהמתקיף מוצא j כך ש- $C^{e^j} \equiv C \pmod N$.

הוכיחו כי $C^{e^{j-1}} \equiv M \pmod N$, כלומר המתקיף מצליח לפענח את הקריפטוגרמה.
מהי סיבוכיות ההתקפה כפונקציה של N ו-k?

שאלה 4 [22 נקודות]

בשאלה זו נתאר פרוטוקול של רבין הנקרא Oblivious Transfer (שליחה אדישה). בפרוטוקול זה ישנם שני משתתפים אליס ובוב.

אליס: בוחרת שני ראשוניים גדולים יהיו p ו-q ומחשבת $N = pq$, ושולחת את N לבוב.

בוב: מגריל a בהתפלגות אחידה מתוך $\mathbb{Z}_N$, מחשב $b = a^2 \bmod N$ ושולח את b לאליס.

אליס: מוציאה שורש ל-b, כלומר מוצאת c כך ש-$b \equiv c^2 \pmod N$, ושולחת את c לבוב.

סעיף א [12 נקודות]

הוכח כי בהסתברות 1/2 בוב יכול לפרק את N בצורה יעילה.

סעיף ב [10 נקודות]

הוכח כי בהסתברות 1/2 בוב לא לומד דבר מהפרוטוקול.