עמוס ביימל
אורי שטמר

אוניברסיטת בן-גוריון בנגב
Ben-Gurion University of the Negev

המחלקה
למדעי המחשב

קריפטוגרפיה – מועד ב'

202-2-5871

סמסטר א' תשע"ו

15.2.2016

הנחיות:

1. בטופס הבחינה 4 עמודים מלבד עמוד זה. ודאו כי כולם נמצאים בידכם.
2. בבחינה 3 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 להתעכב זמן רב מדי על שום סעיף.
7. הנכם רשאים להסתמך על סעיפים קודמים, גם אם לא השבתם עליהם.
8. מותר להסתמך על משפטים שהוכחו בהרצאות, אך יש לצטט אותם במדויק.
9. אם אתם מסתמכים על טענות שהוכחו בתרגילי בית יש להוכיח אותם.
10. **במידה ואינכם יודעים את התשובה לסעיף כלשהו, רשמו "לא יודעים" ותזכו ב- 20% מניקוד הסעיף.**

בהצלחה!

שאלה 1 (30 נקודות)

נסתכל על מערכת חתימה דמוית ElGamal.

<u>יצירת מפתחות</u>

- בחר p ראשוני גדול, ומצא g יוצר של $\mathbb{Z}_p^*$
- הגרל $\boldsymbol{b} \in \mathbb{Z}_{\boldsymbol{p-1}}^*$
- חשב $B = g^b (mod\ p)$
- מפתח פרטי: (p, g, b)
  מפתח ציבורי: (p, g, B)

<u>אלג' הוידוא</u>

קלטים: מפתח ציבורי (p, g, B), מסמך $m \in \mathbb{Z}_{p-1}$, חתימה (γ, δ)

(γ, δ) היא חתימה תקינה על m אם:

- $\boldsymbol{g^{m\delta} B^{\gamma\delta} \equiv \gamma\ (\mathbf{mod}\ p)}$
- $0 \neq \delta \in \mathbb{Z}_{p-1}$, $p - 1 \neq \gamma \in \mathbb{Z}_p^*$

סעיף א [10 נקודות]

הראו כיצד חותם המחזיק במפתח הפרטי יכול לייצר בצורה יעילה חתימה חוקית לכל מסמך $m \in \mathbb{Z}_{p-1}$.
הוכיחו כי החתימה חוקית והסבירו מדוע אלגוריתם החתימה הוא יעיל.
הדרכה: ניתן להיעזר בעובדה שלכל $b \in \mathbb{Z}_{p-1}^*$ ולכל $m \in \mathbb{Z}_{p-1}$, אם מגרילים $\gamma \in \mathbb{Z}_p^*$ בהתפלגות אחידה, אזי $(m + b\gamma) \bmod p - 1$ מתפלג אחיד ב- $\mathbb{Z}_{p-1}$.

סעיף ב [10 נקודות]

הראו כי ללא ההגבלה $p - 1 \neq \gamma$ מתקיף המחזיק במפתח הציבורי יכול ליצר חתימה חוקית לכל מסמך $m \in \mathbb{Z}_{p-1}^*$.

סעיף ג [10 נקודות]

הראו התקפה קיומית על שיטת החתימה בשאלה זו. כלומר הראו איך מתוך המפתח הציבורי אפשר לייצר בצורה יעילה מספר גדול של הודעות וחתימות חוקיות על ההודעות.

שאלה 2 (40 נקודות)

בשאלה זו נבחן את הסכימה הבאה לחלוקת סוד s ל- n משתתפים:

- נתייחס אל הסוד s כוקטור $s \in (\mathbb{Z}_q)^2$ עבור $q > n$ ראשוני. כלומר, $s = (a_1, a_0)$ כאשר $a_0, a_1 \in \mathbb{Z}_q$.
- נגריל $a_2, \dots, a_{t-1} \in \mathbb{Z}_q$ בהתפלגות אחידה באופן ב"ת.
- נגדיר את הפולינום הבא (מדרגה $t-1 \geq$) מעל $\mathbb{Z}_q$: $B(x) = \sum_{i=0}^{t-1} a_i \cdot x^i \ (mod\ q)$.
- עבור $i = 1,2, \dots, n$, החלק של משתתף i הוא $s_i = B(i)$.

סעיף א [3 נקודות]

הראו כי גודל החלק של כל משתתף מקיים $|s_i| = |s|/2$.

סעיף ב [7 נקודות]

הראו כי כל קבוצה של t משתתפים יכולה לשחזר את הסוד.

סעיף ג [10 נקודות]

תהי $I = \{i_1, i_2, \dots, i_{t-2}\}$ קבוצת (אינדקסים של) שחקנים.
הראו כי לכל קביעה של חלקים $s_{i_1}, s_{i_2}, \dots, s_{i_{t-2}}$ עבור שחקנים אלו, ולכל קביעה של הסוד (a_1, a_0), קיים פולינום P מדרגה לכל היותר $t-3$ כך שלכל $i_j \in I$ מתקיים
$$P(i_j) = (s_{i_j} - a_1 \cdot i_j - a_0)/{i_j}^2.$$

סעיף ד [10 נקודות]

תהי $I = \{i_1, i_2, \dots, i_{t-2}\}$ קבוצת (אינדקסים של) שחקנים.
הראו כי לכל קביעה של חלקים $s_{i_1}, s_{i_2}, \dots, s_{i_{t-2}} \in \mathbb{Z}_q$ עבור שחקנים אלו, ולכל קביעה של הסוד $(a_1, a_0) \in (\mathbb{Z}_q)^2$, קיים פולינום Q מדרגה לכל היותר $t-1$ המקיים:

1. המקדם של x^0 (כלומר האיבר החופשי) בפולינום Q הוא a_0
2. המקדם של x^1 בפולינום Q הוא a_1
3. לכל $i_j \in I$ מתקיים $Q(i_j) = s_{i_j}$

סעיף ה [10 נקודות]

הוכיחו כי כל קבוצה של $t-2$ משתתפים לא לומדת דבר על הסוד.
רמז: ניתן להשתמש בעובדה כי הפולנום שמצאתם בסעיף הקודם הוא יחיד.

שאלה 3 (30 נקודות)

נתונה מערכת הצפנה במפתח פומבי $\pi = (Gen, Enc, Dec)$. היזכרו בהגדרת הבטיחות שניתנה בכיתה:

משחק הבחנה א' (עם פרמטר n):

1. $(PK, SK) \leftarrow Gen(1^n)$.
2. בהינתן קלט PK, היריב $\mathcal{A}$ פולט זוג מסרים m_0, m_1 ממרחב המסרים של מערכת ההצפנה.
3. מגרילים בהתפלגות אחידה $b \in \{0,1\}$, ומחשבים קריפטוגרמה $c \leftarrow Enc(m_b, PK)$.
4. היריב $\mathcal{A}$ מקבל את הקריפטוגרמה c ופולט $\hat{b} \in \{0,1\}$. היריב $\mathcal{A}$ מנצח אם $\hat{b} = b$.

הגדרה א':

המערכת π היא בטוחה אם לכל יריב פולינומי הסתברותי $\mathcal{A}$ קיימת פונקציה זניחה $\text{negl}(\cdot)$ כך ש-

$$\Pr\left[\begin{matrix}\text{מנצח } \mathcal{A} \\ \text{במשחק א'}\end{matrix}\right] \leq \frac{1}{2} + \text{negl}(n).$$

בעבודת הבית בחנו את השינויי הבא להגדרת הבטיחות:
במקום לאפשר ליריב לבחור זוג מסרים m_0, m_1, נאפשר לו לבחור רק מסר אחד m. על מנת לנצח במשחק היריב יידרש להבחין בין הצפנה של m לבין הצפנה של $\mathbf{1}$ (הניחו כי $\mathbf{1}$ נמצא במרחב המסרים של המערכת). באופן פורמלי:

משחק הבחנה ב' (עם פרמטר n):

1. $(PK, SK) \leftarrow Gen(1^n)$.
2. בהינתן קלט PK, היריב $\mathcal{B}$ פולט מסר m ממרחב המסרים של מערכת ההצפנה.
3. מגרילים בהתפלגות אחידה $b \in \{0,1\}$.
   אם $b = 0$ אז מחשבים קריפטוגרמה $c \leftarrow Enc(m, PK)$.
   אם $b = 1$ אז מחשבים קריפטוגרמה $c \leftarrow Enc(\mathbf{1}, PK)$.
4. היריב $\mathcal{B}$ מקבל את הקריפטוגרמה c ופולט $\hat{b} \in \{0,1\}$. היריב $\mathcal{B}$ מנצח אם $\hat{b} = b$.

הגדרה ב':

המערכת π היא בטוחה אם לכל יריב פולינומי הסתברותי $\mathcal{B}$ קיימת פונקציה זניחה $\text{negl}(\cdot)$ כך ש-

$$\Pr\left[\begin{matrix}\text{מנצח } \mathcal{B} \\ \text{במשחק ב'}\end{matrix}\right] \leq \frac{1}{2} + \text{negl}(n).$$

בעבודת הבית ראינו כי אם π אינה בטוחה לפי הגדרה ב' אזי π אינה בטוחה לפי הגדרה א'. בשאלה זו נראה שגם הכיוון השני נכון. לצורך כך, בסעיפים הבאים הניחו כי קיים יריב $\mathcal{A}$ המנצח במשחק א' בהסתברות בדיוק $\frac{1}{2} + \epsilon(n)$ עבור $\epsilon(\cdot)$ פונק' <u>לא</u> זניחה, והתבוננו באלגוריתם $\mathcal{B}$ הבא (בו חסר צעד 5).

אלגוריתם $\mathcal{B}$ (מקבל קלט PK):

1. הפעל את $\mathcal{A}$ על PK וקבל זוג הודעות m_0, m_1.
2. הגרל בהתפלגות אחידה $d \in \{0,1\}$.
3. הזן את m_d למשחק ב' וקבל קריפטוגרמה c.
4. הזן את הקריפטוגרמה c ל- $\mathcal{A}$ וקבל $\hat{d}$.
5.

סעיף א [10 נקודות]

חשבו על מהלך המשחק של אלגוריתם $\mathcal{B}$ הנ"ל מול משחק ב', תחת ההנחה כי בשלב 3 של משחק ב' ערכו של b נקבע להיות 1 (כלומר, בשלב 4 של אלגוריתם $\mathcal{B}$ הקריפטוגרמה c היא הצפנה של $\mathbf{1}$). הסבירו מדוע תחת הנחה זו מתקיים ש- $\hat{d} = d$ בהסתברות בדיוק חצי (כאשר $d, \hat{d}$ מוגדרים בשלבים 2,4 של אלגוריתם $\mathcal{B}$ בהתאמה).

סעיף ב [10 נקודות]

חשבו על מהלך המשחק של אלגוריתם $\mathcal{B}$ הנ"ל מול משחק ב', תחת ההנחה כי בשלב 3 של משחק ב' ערכו של b נקבע להיות 0. הסבירו מדוע תחת הנחה זו מתקיים ש- $\hat{d} = d$ בהסתברות בדיוק $\frac{1}{2} + \epsilon(n)$.

סעיף ג [10 נקודות]

השלימו את השורה החסרה באלגוריתם $\mathcal{B}$ כך ש- $\mathcal{B}$ מנצח במשחק ב' בהסתברות $\frac{1}{2} + \frac{\epsilon(n)}{2}$. הוכיחו תשובתכם.

בהצלחה!