2.1.2015

קריפטוגרפיה: תרגיל 5

הגשה: יום ה' 22.1.15 לתא 78 בקומה 1 בניין 37 (שימו לב שרשום על התא "אורי שטמר").
ההגשה בזוגות או ביחידים.

שאלה 1

בשאלה זו תראו מתקפה על שיטת החתימה Textbook RSA.

סעיף א
הראו איך בהינתן המפתח הפומבי (N,e) והודעה אקראית $m \in \mathbb{Z}_N^*$ ניתן לזייף (ביעילות) חתימה על m. לתוקף מותר לבקש חתימה על הודעה אחת (שונה מ- m).

סעיף ב
הסבירו מדוע (תחת הנחת הקושי של RSA) לא ניתן לבצע את הנ"ל מבלי לבקש אף חתימה.

שאלה 2

סעיף א
נתון מאגר נתונים $X \in \{0,1\}^n$, כשאר הביט x_i מייצג מידע פרטי של אדם i.

סטודנט בקורס הציע את האלגוריתם הבא:
בקלט X, בחר $1 \le i \le n$ בהתפלגות אחידה, והחזר את x_i (השורה ה-i -ית ב- X).

הסטודנט טען שהאלג' הנ"ל משמר פרטיות מכיוון שגם אם המידע שלי נמצא ב X, ההסתברות שהמידע שלי ייחשף היא לכל היותר $1/n$.

הוכיחו כי האלג' הנ"ל אינו מקיים ϵ-פרטיות-דיפרנציאלית (לאף ערך של ϵ).

סעיף ב
נתון מאגר נתונים $X \in \{0,1\}^n$, כשאר הביט x_i מייצג מידע פרטי של אדם i.
בכיתה ראינו כי האלג' הבא מקיים ϵ-פרטיות-דיפרנציאלית.

1. הגרל $Y \sim \mathrm{Lap}\left(\frac{1}{\epsilon}\right)$.
2. חשב והחזר $Y + \sum_{i=1}^{n} x_i$.

הסבירו מדוע זה נכון גם עבור האלג' הבא:

1. הגרל $Y \sim \mathrm{Lap}\left(\frac{1}{\epsilon}\right)$.
2. חשב והחזר $Y - \sum_{i=1}^{n} x_i$.

סעיף ג
סטודנט בקורס גילה ששני האלג' הנ"ל מקיימים ϵ-פרטיות-דיפרנציאלית, ולכן טען שהאלג' הבא מקיים 2ϵ-פרטיות-דיפרנציאלית. הוכיחו כי הסטודנט טעה.

1. הגרל $Y \sim \mathrm{Lap}\left(\frac{1}{\epsilon}\right)$.
2. חשב והחזר את $\left(Y + \sum_{i=1}^{n} x_i\right)$ ואת $\left(Y - \sum_{i=1}^{n} x_i\right)$.

שאלה 3

מערכת הצפנה עם מפתח פרטי (E, D, Gen) נקראת <u>נכונה</u> אם כל הודעה m המוצפנת במפתח מפוענחת במפתח ל- m. מערכת הצפנה עם מפתח פרטי (E, D, Gen) נקראת <u>בטוחה</u> אם היא בטוחה על פי ההגדרה שניתנה בכיתה.

סעיף א

נתונות 2 מערכות הצפנה עם מפתח פרטי: (E_1, D_1, Gen_1), (E_2, D_2, Gen_2).
ידוע כי שתיהן נכונות, אך בדיוק אחת מהן בטוחה. לא ידוע מי מהן היא המערכת הבטוחה. בנוסף, נתונה סכמה לחלוקת סוד 2 מתוך 2. מוצעת מערכת ההצפנה הבאה:

- **יצירת מפתחות:**
  הרץ Gen_1 לקבלת k_1, הרץ Gen_2 לקבלת k_2.
  המפתח הסודי: (k_1, k_2).
- **הצפנה של הודעה m:**
  חלק את m על פי סכמה לחלוקת סוד 2 מתוך 2. נסמן את החלקים ב- s_1, s_2.
  חשב $C_1 \leftarrow Enc_1(s_1, k_1)$ ו- $C_2 \leftarrow Enc_2(s_2, k_2)$
  פלוט את ההצפנה $C = (C_1, C_2)$.

הראו כיצד לפענח הודעה במערכת והסבירו מדוע המערכת הנ"ל היא נכונה, ומדוע היא בטוחה.

סעיף ב

נתונות 3 מערכות הצפנה. ידוע שלפחות 2 מהן נכונות ושלפחות 2 מהן בטוחות. לא ידוע איזה מהן בטוחות ואיזה מהן נכונות. הראו מערכת הצפנה העונה על הדרישות הבאות:

1. המערכת משתמשת רק במערכות הצפנה הנתונות ובסכמת חלוקת סוד לפי בחירתכם.
2. המערכת בטוחה.
3. מפענח אשר יודע אילו מבין שלושת המערכות הן הנכונות, יכול לפענח הצפנות (המצפין <u>לא</u> יודע מיהן הנכונות ומיהן הבטוחות).

הסבירו מדוע המערכת שבניתם עונה לדרישות 2 ו- 3.

סעיף ג

נתונות 5 מערכות הצפנה. ידוע שלפחות 4 מהן נכונות ושלפחות 4 מהן בטוחות. לא ידוע איזה מהן בטוחות ואיזה מהן נכונות. הראו מערכת הצפנה נכונה ובטוחה המשתמשת רק במערכות הצפנה הנתונות ובסכמת חלוקת סוד לפי בחירתכם.
<u>שימו לב</u>: כאן גם המצפין וגם המפענח לא יודעים מיהן המערכות הבטוחות ומיהן המערכות הנכונות.

הסבירו מדוע המערכת שבניתם עונה לדרישות.

שאלה 4

נתון פרוטוקול ה- OT הבא. **קלטים:** בוב מחזיק $x_0, x_1 \in \{0,1\}$. אליס מחזיקה $s \in \{0,1\}$.

<u>תחילה אליס מבצעת:</u>

- מגרילה q ראשוני כך ש- $p = 2q + 1$ ראשוני, ומוצאת $h \in \mathbb{Z}_p$ שהסדר שלו הוא q.
- מגרילה $b \in \mathbb{Z}_q$ באקראי.
- אם $s = 0$ אזי:
  מחשבת $B_0 = h^b \bmod p$
  מגרילה $B_1 \in QR_p$ באקראי
- אם $s = 1$ אזי:
  מגרילה $B_0 \in QR_p$ באקראי
  מחשבת $B_1 = h^b \bmod p$
- שולחת לבוב את p, h, B_0, B_1.

<u>לאחר מכן בוב מבצע:</u>

- מגריל $a_0, a_1 \in \mathbb{Z}_q$ באקראי.
- מחשב עבור $i \in \{0,1\}$:

$$A_i = h^{a_i} \bmod p$$
$$C_i = B_i^{a_i} \cdot h^{x_i} \bmod p$$

- שולח לאליס את A_0, C_0, A_1, C_1.

סעיף א

איך אליס משחזרת את הביט x_s?

סעיף ב

הוכיחו כי בוב לא לומד שום מידע על s.

סעיף ג

הסבירו מדוע אליס לא לומדת שום מידע על x_{1-s}. מותר להסתמך על בטיחות מערכת ההצפנה של $ElGamal$.

סעיף ד

הוכיחו כי אם אליס רמאית אז היא יכולה ללמוד בצורה יעילה את שני הביטים.

שאלה 5

השרת מחזיק מאגר נתונים - $\vec{X} = (x_1, x_2, \dots x_n)$, כאשר $x_i \in \{0,1\}$.
משתמש מעוניין לדעת מהו x_i עבור $1 \leq i \leq n$ מסוים.

בכיתה ראינו פרוטוקול PIR עם 2 שרתים וסיבוכיות תקשורת $O(\sqrt{n})$. בשאלה זו נתכנן פרוטוקול עם 4 שרתים וסיבוכיות תקשורת $O(n^{1/3})$.

סעיף א

הראו פרוטוקול עם 2 שרתים בו אורך השאילתא הוא $O(n^{1/3})$ ואורך התשובה הוא $O(n^{2/3})$.
הסבירו את נכונות ובטיחות הפרוטוקול.

סעיף ב

שימו לב שבפרוטוקול שתכננתם בסעיף הקודם המשתמש היה צריך רק ביט אחד מתוך כל אחת מהתשובות. השתמשו בעובדה זו והראו פרוטוקול עם 4 שרתים וסיבוכיות תקשורת $O(n^{1/3})$.
הסבירו את נכונות ובטיחות הפרוטוקול.

<u>רמז</u>: השתמשו בפרוטוקול מהסעיף הקודם וסמלצו כל אחד מהשרתים בו ע"י 2 שרתים.