31.12.2015

קריפטוגרפיה: תרגיל 5

<u>הגשה</u>: יום ד' 20.1.16 בשעה 14:10 בהרצאה. ההגשה בזוגות או ביחידים.

שאלה 1

נתאר מערכת חתימה:

- אלגוריתם יצירת המפתחות זהה לאלגוריתם יצירת המפתחות במערכת החתימה של ElGamal. כלומר, בוחרים p ראשוני, g יוצר של $\mathbb{Z}_p^*$ ו- $b \in \{1, \dots, p-2\}$, ומחשבים $B \leftarrow g^b \bmod p$. מפתח החתימה הפרטי הוא (p, g, b) ומפתח הוידוא הציבורי הוא (p, g, B).
- תחום ההודעות הוא $\mathbb{Z}_{p-1}^*$.
- כדי לחתום על מסמך M מוצאים z כך ש- $z \cdot M \equiv b \pmod{p-1}$, והחתימה היא $S \leftarrow g^z \bmod p$
- אלגוריתם הוידוא מכריז כי S היא חתימה חוקית על מסמך M אם"ם $S^M \equiv B \pmod{p}$

תזכורת: חתימה היא חוקית אם אלגוריתם הוידוא מכריז כי חתומה זו חוקית.

סעיף א

הראו כי אלגוריתם הוידוא תקין, כלומר אם החתימה S חושבה ע"י אלגוריתם החתימה אזי החתימה חוקית.

סעיף ב

מערכת חתימה זו אינה בטוחה. הראו כיצד זייפן יכול לייצר חתימה חוקית לכל הודעה $M \in \mathbb{Z}_{p-1}^*$.

שאלה 2

נסתכל על הסכמה הבאה לחלוקת סוד t-מתוך-n. יהי p ראשוני כך ש- $p > n$. לחלק סוד $s \in \mathbb{Z}_p$, המחלק מגריל $t-1$ איברים אקראיים $r_0, r_1, \dots, r_{t-2}$ מתוך $\mathbb{Z}_p$, מסתכל על הפולינום

$$Q(x) = \left(s \cdot x^{t-1} + \sum_{j=0}^{t-2} r_j \cdot x^j \right) \bmod p$$

ונותן למשתתף i את החלק $Q(i)$. שימו לב כי הסוד הוא המקדם של x^{t-1}.

סעיף א

הראו כי כל קבוצה של משתתפים בגודל לפחות t יכולה לשחזר את הסוד בצורה יעילה מתוך החלקים שקיבלה.

סעיף ב

נסתכל על הפולינום $R(x) = \left(\sum_{j=0}^{t-2} r_j \cdot x^j\right) \bmod p$. הוכיחו כי אם משתתף i יודע מהו הסוד, אזי הוא יכול לחשב את $R(i)$ מתוך $Q(i)$.

סעיף ג

הוכיחו כל כל קבוצה בגודל $t-1$ לא מקבלת מידע על הסוד מתוך החלקים שלה, כלומר, בהינתן החלקים כל סוד $s \in \mathbb{Z}_p$ אפשרי.

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

יהי $T > 0$ שלם, ויהי $X = (x_1, x_2, \dots, x_n) \in \{1,2, \dots, T\}^n$ דטהבייס המכיל n מספרים בין 1 ל- T.
לכל $1 \le j \le T$ נסמן את מספר האיברים בדטהבייס הגדולים שווים ל- j כ- $f_j(X) = |\{i : x_i \ge j\}|$.

סעיף א

תכננו אלגוריתם $\mathcal{A}_j$ המשמר ε/T פ"ד אשר בקלט X מחזיר הערכה רועשת a_j ל- $f_j(X)$. חשבו את גודל הדהבייס n הדרוש על מנת ש-

$$\Pr\left[\left|a_j - f_j(X)\right| \le \frac{n}{100}\right] \ge 1 - \frac{1}{100T}$$

סעיף ב

תכננו אלגוריתם המשמר ε פ"ד אשר בקלט X מחזיר הערכות רועשת $a_1, \dots, a_T$ ל- $f_1(X), \dots, f_T(X)$. חשבו את גודל הדהבייס n הדרוש על מנת ש-

$$\Pr\left[\forall j : \left|a_j - f_j(X)\right| \le \frac{n}{100}\right] \ge 1 - \frac{1}{100}$$