קריפטוגרפיה – מועד ב'

202-2-5871
סמסטר א' תשע"ד
10.2.2014

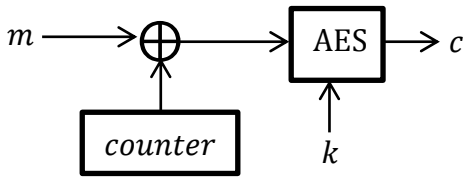
הנחיות:

1. בטופס הבחינה 3 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 [35 נקודות]

ניזכר בשיטת ההצפנה ע"י CBS עם מונה עבור הודעה של בלוק אחד:



כלומר $c = \mathrm{AES}(m \oplus counter\,, k)$, כאשר לאחר כל פעולת הצפנה ערך המונה מקודם ב- 1.

נתונה הודעה m_0, ונתונה הצפנה c של הודעה m כלשהי (לא ידועה). נסמן ב- y את ערך המונה שאיתו הוצפנה ההודעה m. בשני הסעיפים הבאים תראו כי בתנאים מסויימים מתקיף יכול להבחין ביעילות האם $m = m_0$ או לא.

<u>הערות עבור שני הסעיפים:</u>

- y הוא ערך המונה אשר איתו הוצפנה ההודעה m.
- כשהמתקיף מבקש לראות הצפנה של הודעה כלשהי, ערך המונה יהיה $(y + 1)$.

סעיף א [18 נקודות]

הראו כי מתקיף אשר יודע את y יכול להכריע ביעילות האם $m = m_0$ או לא. למתקיף מותר לבקש הצפנה עבור הודעה אחת ששונה מ- m_0.

סעיף ב [17 נקודות]

הראו כי מתקיף אשר יודע ש- y זוגי יכול להכריע ביעילות האם $m = m_0$ או לא (כעת המתקיף איננו יודע את y, אלא רק יודע שהוא זוגי). כמו בסעיף הקודם, למתקיף מותר לבקש הצפנה עבור הודעה ששונה מ- m_0.

שאלה 2 [15 נקודות]

היזכרו בהתקפה שראינו בכיתה על שימוש ב Textbook RSA להצפנת מסרים קצרים: בהצפנת מסר m כך ש- $m < N^{1/e}$ (כאשר (N, e) הוא המפתח הפומבי), נקבל:

$$c = m^e \ (mod\ N) = m^e \quad \longleftarrow \text{מעל השלמים}$$

(ומעל השלמים אפשר לחשב שורש e-י ביעילות).

אליס רוצה לשלוח לבוב הודעה קצרה $m < N^{1/e}$, ובמטרה להימנע מההתקפה הנ"ל, היא שולחת לו הצפנה של $m' = 2^{100} \cdot m$.

הראו כיצד יריב אשר יודע כי אליס שולחת הצפנה של $m' = 2^{100} \cdot m$ עבור $m < N^{1/e}$ יכול לתקן את המתקפה הנ"ל ולפענח ביעילות את m.

שאלה 3 [50 נקודות]

היזכרו במשחק **DDH** שהגדרנו בכיתה:

1. הגרל ראשוני q בן k ביטים כך שגם $p = 2q + 1$ ראשוני.
2. בחר g יוצר של $\mathbb{Z}_p^*$ וסמן $h = g^2 (mod\ p)$.
3. הגרל בהתפלגות אחידה $a, b \in \mathbb{Z}_q$ וחשב
$$A = h^a\ (mod\ p)$$
$$B = h^b\ (mod\ p)$$
4. הגרל $d \in \{0,1\}$ בהתפלגות אחידה.
אם $d = 1$ אזי חשב $C = h^{ab}\ (mod\ p)$.
אחרת הגרל $C \in QR_p$ בהתפלגות אחידה.
5. היריב $\boldsymbol{\mathcal{A}}$ מופעל על p, h, A, B, C ופולט $\hat{d}$.
$\boldsymbol{\mathcal{A}}$ מנצח אם $d = \hat{d}$.

הנחת הקושי של DDH:
לכל אלגוריתם פולינומי הסתברותי $\boldsymbol{\mathcal{A}}$ קיימת פונקציה זניחה $\mathrm{negl}(\cdot)$ כך ש-
$$\Pr\begin{bmatrix}\text{מנצח } \boldsymbol{\mathcal{A}} \\ \text{במשחק DDH}\end{bmatrix} \leq \frac{1}{2} + \mathrm{negl}(k)$$

<u>נגדיר משחק newDDH באופן הבא:</u>

1. הגרל ראשוני q בן k ביטים כך שגם $p = 2q + 1$ ראשוני.
2. בחר g יוצר של $\mathbb{Z}_p^*$ וסמן $h = g^2 (mod\ p)$.
3. הגרל בהתפלגות אחידה $a, b \in \mathbb{Z}_q$ וחשב
$$A = h^a\ (mod\ p)$$
$$B = h^b\ (mod\ p)$$
4. הגרל $d \in \{0,1\}$ בהתפלגות אחידה.
אם $d = 1$ אזי חשב $C = h^{ab}\ (mod\ p)$.
אחרת חשב $C = h^{ab+1}\ (mod\ p)$.
5. היריב $\boldsymbol{\mathcal{A}}$ מופעל על p, h, A, B, C ופולט $\hat{d}$.
$\boldsymbol{\mathcal{A}}$ מנצח אם $d = \hat{d}$.

סעיף א [10 נקודות]

הוכיחו כי תחת הנחת הקושי של DDH, לכל אלגוריתם פולינומי הסתברותי $\boldsymbol{\mathcal{A}}$ קיימת פונקציה זניחה $\mathrm{negl}(\cdot)$ כך ש-
$$\Pr\begin{bmatrix}\text{מנצח } \boldsymbol{\mathcal{A}} \\ \text{במשחק newDDH}\end{bmatrix} \leq \frac{1}{2} + \mathrm{negl}(k)$$

בסעיפים הבאים נבחן את הנכונות והבטיחות של פרוטוקול החישוב הבטוח הבא.

עבור $(\boldsymbol{x_1}, \dots, \boldsymbol{x_n}) \in \{\boldsymbol{0}, \boldsymbol{1}\}^{\boldsymbol{n}}$ ו- $(\boldsymbol{y_1}, \dots, \boldsymbol{y_n}) \in \{\boldsymbol{0}, \boldsymbol{1}\}^{\boldsymbol{n}}$, נגדיר פונקציה $\boldsymbol{f}$ באופן הבא:

$$f\big((x_1, \dots, x_n), (y_1, \dots, y_n)\big) = \sum_{i=1}^{n} x_i y_i$$

כלומר $f: \{0,1\}^n \times \{0,1\}^n \to \{0,1,2, \dots, n\}$. נתאר פרוטוקול חישוב בטוח עבור f באופן הבא.

<u>קלטים</u>: אליס מחזיקה $\vec{x} = (x_1, \dots, x_n) \in \{0,1\}^n$. בוב מחזיק $\vec{y} = (y_1, \dots, y_n) \in \{0,1\}^n$.

<u>תחילה אליס מבצעת:</u>

- מגרילה $q > n$ ראשוני כך שגם $p = 2q + 1$ ראשוני.
- מוצאת יוצר g של $\mathbb{Z}_p^*$ ומחשבת $h = g^2 \ (mod\ p)$.
- מגרילה $a, b_1, b_2, \dots, b_n \in \mathbb{Z}_q$ בהתפלגות אחידה ומחשבת $A = h^a \ (mod\ p)$.
- לכל $1 \le i \le n$ מחשבת:

$$c_i = ab_i + x_i \ (mod\ q)$$
$$B_i = h^{b_i} \ (mod\ p)$$
$$C_i = h^{c_i} \ (mod\ p)$$

- אליס שולחת לבוב את $p, h, A, B_1, C_1, B_2, C_2, \dots, B_n, C_n$.

<u>לאחר מכן בוב מבצע:</u>

- מחשב $B = \prod_{\{i:y_i=1\}} B_i \ (mod\ p)$ ו- $C = \prod_{\{i:y_i=1\}} C_i \ (mod\ p)$.
- שולח B, C לאליס.

סעיף ב [10 נקודות]

הוכיחו כי $C = B^a \cdot h^{f(\vec{x},\vec{y})} \ (mod\ p)$.

סעיף ג [10 נקודות]

הראו כיצד אליס יכולה לחשב את $f(\vec{x}, \vec{y})$ בצורה יעילה, כלומר בזמן פולינומי ב- n וב- $\log p$.

סעיף ד [10 נקודות]

תחת הנחת הקושי של newDDH, הסבירו מדוע בוב לא לומד מידע על $\vec{x}$.

סעיף ה [10 נקודות]

הראו כיצד אליס הגונה יכולה לבדוק האם $\vec{y} = (1,0,0,0, \dots, 0)$.