מבוא לקריפטוגרפיה מודרנית (0368-3049)

נכתב ע"י רון גולדמן
ע"פ הרצאות של פרופ' בני אפלבאום

1 בנובמבר 2025

תוכן העניינים

1 מבוא **2**

1.1 הגדרות ומושגים ראשונים 2

1.2 דוגמאות 3

1.3 התקפה כללית (נראות מירבית) 4

פרק 1

מבוא

1.1 הגדרות ומושגים ראשונים

1.1.1 מערכת הצפנה

הגדרה 1.1 [פונקצית הצפנה]. $E : \mathcal{K} \times \mathcal{M} \to \mathcal{C}$, לכל $k \in \mathcal{K}, m \in \mathcal{M}$ נסמן $E_k(m) = E(k, m) = c \in \mathcal{C}$ ה-**ciphertext**.

הגדרה 1.2 [פונקצית פיענוח]. $D : \mathcal{K} \times \mathcal{C} \to \mathcal{M}$, לכל $k \in \mathcal{K}, c \in \mathcal{C}$ נסמן $D_k(c) = D(k, c) = m \in \mathcal{M}$ ה-**plaintext**.

הגדרה 1.3 [נכונות]. לכל הודעה $m \in \mathcal{M}$ ומפתח $k \in \mathcal{K}$ מתקיים $D_k(E_k(m)) = m$.

הגדרה 1.4 [מערכת הצפנה סימטרית]. מערכת הצפנה שבה משתמשים במפתח יחיד לצורך הצפנה ופיענוח.

הערה 1.5.

- המפתח $k \sim \mathrm{Unif}(\mathcal{K})$.
- מרחב ההודעות $\mathcal{M} = \{0,1\}^*$.
- הרבה פעמים אורך ההודעות קשור למרחב המפתחות.

1.1.2 מודל התקשורת

- שתי צדדים - אליס ובוב
- קו תקשורת אמין
- סכמת הצפנה משותפת: E, D, k.
- מטרה: לשלוח בבטיחות הודעה m.

1.1.3 מטרות אבטחה

יש מספר מטרות שנרצה להשיג

- אף יריב לא יכול לקבוע את m
- אף יריב לא יכול לקבוע אף אינפורציה לגבי m
- אף יריב לא יכול לקבוע אינפורציה משמעותית לגבי m

שאלות חשובות:

- מה היריב יודע מראש?
- מה המגבלות החישוביות של היריב?

האם בכלל אפשר לפרמל מתמטית את מושג הסודיות?

1.1.4 מודל היריב: מאזין פאסיבי

איב מאזינה לערוץ התקשורת.

- איב מנסה לגלות אינפורציה לגבי m
- איב יודעת את האלגוריתמים E, D (עיקרון קרכהוף)
- איב יודעת את מרחב ההודעות
- איב תפסה את $E_k(m)$
- איב לא יודעת את k

1.2 דוגמאות

דוגמה 1.6 [צופן קיסר].
- מפתח: $k \in \{0, 1, \ldots, 25\}$.
- כל אות מיוצגת כמספר $p \in \{0, 1, \ldots, 25\}$.
- הצפנה: $E_k(p) = p + k \bmod 26$.
- פיענוח: $D_k(p) = p - k \bmod 26$.
- פתרון: חיפוש ממצה.
- מסקנה: דרוש מרחב מפתחות גדול.

דוגמה 1.7 [צופן החלפה].
- מפתח: תמורה $\sigma : [26] \hookrightarrow [26]$.
- כל אות מיוצגת כמספר $p \in \{0, 1, \ldots, 25\}$.
- הצפנה: $E_\sigma(p) = \sigma(p)$.
- פיענוח: $D_\sigma(p) = \sigma^{-1}(p)$.
- יש $26! \approx 4 \cdot 10^{27}$ מפתחות ולכן חיפוש ממצה לא יעבוד.
- ניתן לשבור את ההצפנה באמצעות סטטיסטיקות של שפה טבעית, שכן התדירות שימוש לא אחידה.

דוגמה 1.8 [הצפנת ויז'נר]. המפתח הוא beads:

t	h	e	m	a	n	a	n	d	t	h	e	w	o	m	a	n
b	e	a	d	s	b	e	a	d	s	b	e	a	d	s	b	e
V	M	F	Q	T	P	F	O	H	M	J	J	X	S	F	C	S

- האם הוא מאובטח?
- ויז'נר: אני לא מצליח לשבור אותו אז הוא מאובטח.
- קסיסיקי (1863): שבר אותו.

1.3 התקפה כללית (נראות מירבית)

ליריב יש מידע מקדים על ההודעות, הנתונה כהתפלגות M על מרחב ההודעות $\mathcal{M}$.
בהינתן סייפרטקסט $C = E_k(M) \xleftarrow{R} \mathcal{K}$, עשה:

- פענח לכל מפתח אפשרי:

$$D_{000}(C) = \text{blabla}, D_{001}(C) = \text{lunch}, \ldots, D_{111}(C) = \text{attack}$$

- בהתבסס על ההתפלגות M בחר את ההודעה הכי סבירה

שאלה: האם ניתן להביס כזה יריב?

1.3.1 בטיחות מושלמת

הגדרה 1.9 [פילוגים שווים]. $X \equiv Y$ עבור התפלגויות מעל $\mathcal{D}$ אם

$$\forall d \in \mathcal{D}.\ \Pr[X = d] = \Pr[Y = d]$$

הגדרה 1.10 [בטיחות מושלמת (שאנון 1949)]. מתקיים $M|C \equiv M$.

הגדרה 1.11 [בטיחות - הגדרה אלטרנטיבית]. מתקיים כי לכל $m_0, m_1 \in \mathcal{M}$ באורך זהה, לכל $c \in \mathcal{C}$

$$\Pr_{k \xleftarrow{R} \mathcal{K}}[E_k(m_0) = c] = \Pr_{k \xleftarrow{R} \mathcal{K}}[E_k(m_1) = c]$$

כלומר $C|M \equiv C$.

דוגמה 1.12 [פנקס חד-פעמי].

- מרחב ההודעות $\mathcal{M} = \{0,1\}^n$
- מרחב המפתחות $\mathcal{K} = \{0,1\}^n$. המפתח נבחר באקראי.
- כדי להצפין/לפענח נחשב XOR של ההודעה/הטקסט המצופן עם המפתח:

$$\begin{aligned} E_k(m) =& m \oplus k \\ D_k(c) =& c \oplus k \end{aligned}$$

הערה 1.13. להשתמש במפתח רק פעם אחת! אחרת נקבל ויז'נר.

משפט 1.14. לפנקס חד-פעמי יש בטיחות מושלמת. כלומר, לכל $m_0, m_1 \in \{0,1\}^n$ מתקיים $E_k(m_0) \equiv E_k(m_1)$, כאשר $k \xleftarrow{R} \mathcal{K}$.

הוכחה. מספיק להוכיח את הטענה הבאה:

טענה 1.15. לכל $m, c \in \{0,1\}^n$ מתקיים

$$\Pr_{k \xleftarrow{R} \mathcal{K}}[E_k(m) = c] = \frac{1}{2^n} \iff E_k(m) \sim U_n$$

הטענה גוררת את המשפט כי מטרנזטיביות שוויון ההתפלגות לכל $m_0, m_1 \in \{0,1\}^n$ מתקיים

$$E_k(m_0) \equiv U_n \equiv E_k(m_1)$$

כעת נוכיח את הטענה.
נקבע $m, c \in \{0,1\}^n$, אזי:

$$\Pr_k[E_k(m) = c] = \Pr_k[m \oplus k = c] = \Pr_k[k = m \oplus c] = \frac{1}{2^n}$$

כי $m \oplus c$ קבוע ו-$k \sim U_n$. ■

1.3.2 יתרונות וחסרונות של פנקס חד-פעמי

- יתרון: בטיחות מושלמת.
- בעיה: גודל מרחב המפתחות.

משפט 1.16 [שאנון]. אם מערכת הצפנה $E : \mathcal{K} \times \mathcal{M} \to \mathcal{C}, D : \mathcal{K} \times \mathcal{C} \to \mathcal{M}$ בעלת בטיחות מושלמת, אזי $|\mathcal{K}| \geq |\mathcal{M}|$.

הוכחה. נגדיר גרף דו-צדדי $G = (V, E)$ כאשר $V = \mathcal{M} \uplus \mathcal{C}$ (בה"כ נזהה אותם כמרחבים שונים) ו-$\{m, c\} \in E$ אם ורק אם קיים $k \in \mathcal{K}$ כך ש- $E_k(m) = c$.
נניח בשלילה כי $|\mathcal{K}| < |\mathcal{M}|$, נקבע $\{m, c\} \in E$.

טענה 1.17. c יכול להיות מחובר לכל היותר ל-$|\mathcal{K}|$ הודעות, כלומר $\deg(c) \leq |\mathcal{K}|$.

הוכחת הטענה. נניח בשלילה כי $\deg(c) > |\mathcal{K}|$, אז מעיקרון שובך היונים יש מפתח k ו-$m_0 \neq m_1$ כך ש-$c = E_k(m_0) = E_k(m_1)$ וזו סתירה לנכונות ההצפנה.

מסקנה 1.18. קיימת הודעה m^* כך שאינה שכנה של c.

לכל $k \in \mathcal{K}$, $E_k(m^*) \neq c$, ולכן $\Pr_k[E_k(m^*) = c] = 0$.
משום ש-$\{m, c\} \in E$ אזי יש $k' \in \mathcal{K}$ עבורו $E_{k'}(m) = c$ ולכן $\Pr_k[E_k(m) = c] \geq \frac{1}{|\mathcal{K}|} > 0$.
בפרט מתקיים כי $E_k(m^*) \not\equiv E_k(m)$ וזו סתירה לבטיחות המושלמת. ■