2.03.2021	***קריפטוגרפיה 2***

הרצאה 1: מבוא

Textbook: Katz and Lindell. Introduction to Modern Cryptography.

מרצה: אורי שטמר

מה ההבדלים בין הקורס הזה לקורס הקודם (קריפטוגרפיה שימושית)?

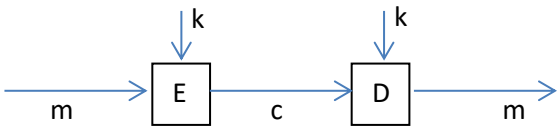
1. הקורס הקודם היה הרבה פחות פורמלי. למשל, בקורס הקודם אמרנו דברים כמו "מערכת חתימה היא בטוחה אם קשה לזייף חתימה". מה זאת אומרת קשה לזייף חתימה? בקורס הזה אנחנו נגדיר בדיוק מה אנחנו מתכוונים כשאנחנו אומרים שמערכת היא בטוחה.

2. הקורס הזה יהיה הרבה יותר אבסטרקטי. למשל, בקורס הקודם ראינו איך לבנות מערכות הצפנה מבעיות ספציפיות כמו למשל RSA או הלוג הדיסקרטי. בקורס הזה (או לפחות ברובו) לא נרצה להסתמך על בעיות ספציפיות, אלא נתעניין בשאלות כלליות יותר, כמו למשל:

"נניח שיש לי פונקציה חד כיוונית (כלשהי). האם אני יכול לבנות ממנה מערכת הצפנה?"

הייתרונות של הגישה הזאת הן:
(א) זה מראה לנו בדיוק על מה מתבססות המערכות שלנו
(ב) אח"כ נוכל לבסס בניה כזאת על כל הנחה ספציפית שנותנת לנו פונקציה חד כיוונית
[חיסרון של הגישה הזאת: בניות המתבססות על הנחות ספציפיות הן יעילות יותר...]

בטיחות חישובית – דוגמה:



הצופן c מכיל אולי אינפורמציה על m, אבל אי אפשר לנצל זאת על ידי חישוב יעיל.
מה זה אומר בדיוק?

זמן הריצה של היריב והשחקנים ההוגנים יהיו פונקציות של פרמטר הבטיחות n (למשל אורך המפתח במערכת הצפנה). נזהה אסטרטגיות פיזביליות עם אלה שזמן החישוב שלהן פולינומי ב- n.

דגשים:

- עבור השחקנים "ההוגנים" זמן החישוב הוא פולינום ב- n שנקבע ע"י תכנון המערכת
- עבור היריבים, זמן החישוב יהיה פולינום כלשהו. למשל, בשביל לשבור את המערכת, היריב עשוי להיות מוכן לרוץ בזמן n^{ℓ} עבור ℓ כלשהו שהוא בחר, כאשר ℓ לא נקבע ע"י מתכנן המערכת. בפרט, זמן הריצה של היריב יכול להיות גדול בהרבה מזמן הריצה של השחקנים ההגונים.
- יריבים/מתקפות שזמן הריצה שלהם אינו חסום ע"י פולינום יחשבו לא ראליים (למשל $n^{\log n}$ או 2^n).
- אנחנו נדבר על אלגוריתמים אקראיים.

<u>הגדרה:</u> אלגוריתם אקראי הוא אלגוריתם אשר בכל צעד יכול להטיל מטבע אקראי ועל סמך התשובה להחליט מה לעשות. הגדרה שקולה: לאלגוריתם אקראי יש 2 קלטים r,x כאשר r מוגרל באקראי.

- למה שנדבר על אקראיות? אקראיות היא <u>הכרחית</u> בקריפטוגרפיה (למשל לבחירת מפתח). בנוסף אקראיות היא מעשית ולכן לא ניתן להניח שליריבים אין אקראיות...

- מה זאת אומרת אלגוריתם <u>אקראי</u> <u>פולינומי</u>?

<u>אפשרות (א):</u> קיים פולינום $p(\cdot)$ כך שלכל x,r זמן הריצה חסום על ידי $p(|x|)$
<u>אפשרות (ב):</u> קיים פולינום $p(\cdot)$ כך שלכל x תוחלת זמן הריצה חסומה על ידי $p(|x|)$

לדוגמה, נסתכל על אלגוריתם שמטיל מטבעות אקראיים ועוצר אחרי שראה $5 \cdot \log n$ מטבעות שהם אפס. ההסתברות ש- $5 \cdot \log n$ מטבעות רצופים יהיו כולם אפסים היא $1/2^{5\log n} = 1/n^5$ ולכן תוחלת זמן הריצה היא לכל היותר $O(n^5 \log n)$, אבל קיימות ריצות שלא עוצרות.

- אמרנו שאנחנו רוצים להתגונן מפני יריבים <u>יעילים</u> חישובית. אבל מה לגבי יריבים אשר בצעו חישוב מקדים ארוך ויקר ולאחר מכן מסוגלים לבצע את התקיפה בצורה יעילה? נרצה (לפעמים) להתגונן גם מפני יריבים כאלה. ליריבים כאלה קוראים יריבים פולינומיים <u>לא-אחידים</u>.

- נרצה להגיד שיריב יעיל, גם אם הוא עשה חישוב מקדים ארוך, לא יוכל לשבור את המערכת. איך נמדל חישוב מקדים כזה? ניתן לאלגוריתם מחרוזת נוספת שתייצג את פלט החישוב המקדים. למחרוזת הזאת קוראים <u>עיצה</u>. אנחנו רוצים לדבר על אסימפטוטיקה ולכן לכל אורך קלט ניתן מחרוזת אחרת (באורך פולינומי באורך הקלט).

<u>הגדרה:</u> אלגוריתם פולימוני <u>לא-אחיד</u> הוא זוג $(M, \bar{a})$ כאשר M הוא אלגוריתם פולינומי המקבל 2 קלטים ו- $\bar{a}$ היא סדרה אינסופית של מחרוזות כך ש- $|a_n| = \text{poly}(n)$. לכל x נחשוב על ההפעלה של M על הזוג $(x, a_{|x|})$.

אז הבנו את היכולות של היריב. הוא רץ בזמן פולינומי והוא יכול להטיל מטבעות. לפעמים נאפשר לו גם לבצע חישוב מקדים, מה שאנחנו ממדלים ע"י אלגוריתם לא-אחיד.

<u>אבל עדיין</u> גם ליריב יעיל יש סיכויי (אמנם קטן אבל קיים) שהוא ישבור את המערכת, למשל אם היריב מנחש את המפתח הסודי. כלומר, אפילו שאנחנו מדברים על יריבים <u>יעילים</u>, לא נוכל לומר שהם לא יכולים לשבור את המערכת <u>אף פעם</u>. מה שכן נוכל לדרוש זה שסיכויי ההצלחה של יריבים יעילים יהיו אומללים.

<u>סיכויי הצלחה של יריבים</u>

נגדיר הסתברות <u>כזניחה</u> אם (כפונקציה של n) היא קטנה אסימפטוטית מ $1/p(n)$ לכל פולינום חיובי $p(\cdot)$.

דוגמה: נחשוב על יריב שמצליח בהסתברות לכל היות $2^{40} \cdot 2^{-n}$ אם הוא רץ בזמן n^3 דקות. אם נבחר $n = 50$ אז היריב רץ בזמן 50^3 דקות (3 חודשים) ומצליח בהסתברות $\approx \frac{1}{1000}$. אם נבחר $n = 500$ אז היריב רץ בזמן 500^3 דקות (200 שנה) ומצליח בהסתברות 2^{-460}.

הגדרה: פונקציה $negl(\cdot)$ תקרא <u>זניחה</u> אם לכל פולינום חיובי $p(\cdot)$ קיים n_0 כל שלכל $n \geq n_0$ מתקיים

$$negl(n) < \frac{1}{p(n)}$$

טענה: אם ν_1, ν_2 הן פונקציות זניחות אזי גם $\nu_3(n) = \nu_1(n) + \nu_2(n)$ זניחה.

הוכחה: יהי $p(\cdot)$ פולינום. מכיוון שגם $2 \cdot p(\cdot)$ הוא פולינום, קיימים n_1, n_2 כך ש-

$$\forall n \geq n_1: \ \ \nu_1(n) < \frac{1}{2 \cdot p(n)}$$
$$\forall n \geq n_2: \ \ \nu_2(n) < \frac{1}{2 \cdot p(n)}$$

נבחר $n_3 = \max\{n_1, n_2\}$ ונקבל:

$$\forall n \geq n_3: \ \ \nu_3(n) = \nu_1(n) + \nu_2(n) < \frac{1}{2 \cdot p(n)} + \frac{1}{2 \cdot p(n)} = \frac{1}{p(n)}$$

מ.ש.ל.

המסר כאן הוא שאם אנחנו מחברים פונקציות זניחות אז אנחנו נשארים עם פנקציות זניחות. (אזהרה – לא לעשות עם זה אינדוקציה).

טענה: אם ν פונקציה זניחה ו- $q(\cdot)$ הוא פולינום חיובי אזי גם $\nu'(n) = q(n) \cdot \nu(n)$ זניחה.

הוכחה: יהי $p(\cdot)$ פולינום חיובי. גם $p \cdot q$ הוא פולינום ולכן קיים n_0 כל שלכל $n \geq n_0$ מתקיים $\nu(n) < \frac{1}{p(n) \cdot q(n)}$, כלומר $\nu'(n) < \frac{1}{p(n)}$.

מ.ש.ל.

עכשיו כשאנחנו מבינים גם מהם סוגי היריבים שנדבר עליהם וגם מהי הסתברות זניחה, נוכל לדבר על מסגרת כללית עבור הגדרות בטיחות:

<u>דוגמה/תבנית להגדרת בטיחות:</u>

מערכת היא <u>בטוחה</u> אם לכל יריב פולינומי אקראי $\mathcal{A}$ המבצע <u>מתקפה</u>, ההסתברות ש- $\mathcal{A}$ <u>מצליח</u> במתקפה היא זניחה.

הערות:

- כדי להשתמש בתבנית הזאת צריך להגדיר למה אנחנו מתכוונים כשאנחנו אומרים <u>מתקפה</u> ולמה אנחנו מתכוונים כשאנחנו אומרים <u>מצליח</u>
- שימו לב: ההגדרה הזאת היא <u>אסימפטוטית</u>. מדוע? כי בהגדרת פונקציה זניחה לא אכפת לנו מה קורה עבור n-ים קטנים. היינו יכולים לרשום את התבנית הזאת בצורה מפורשת כך:

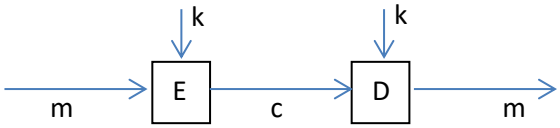
מערכת היא <u>בטוחה</u> אם לכל יריב פולינומי אקראי $\mathcal{A}$ המבצע <u>מתקפה</u> ולכל פולינום חיובי $p(\cdot)$ קיים n_0 כך שלכל $n > n_0$, ההסתברות ש- $\mathcal{A}$ <u>מצליח</u> במתקפה היא קטנה מ- $\frac{1}{p(n)}$.

שימו לב ששום דבר לא מובטח כאן עבור $n \leq n_0$.

אנחנו עדיין צריכים להבין מה זאת אומרת "<u>מתקפה</u>" ומה זאת אומרת "<u>מצליח</u>". זה יהיה תלוי בסוג המערכת שנדבר עליה. למשל, זיוף חתימה זאת משימה שונה מלשבור מערכת הצפנה.

הגדרה פורמלית של בטיחות עבור מערכת הצפנה סימטרית

תזכורת:



מערכת הצפנה סימטרית מורכבת מ-3 אלגוריתמים פולינומיים:

Gen	אלגוריתם אקראי לייצור מפתחות קלט: פרמטר בטיחות 1^n פלט: מפתח k (מתקיים $\|k\| \leq p(n)$ עבור פולינום כלשהו) נסמן $k \leftarrow Gen(1^n)$ בה"כ נניח כי $n \leq \|k\|$
Enc	אלגוריתם אקראי להצפנה קלט: הודעה $m \in \{0,1\}^*$ ומפתח k פלט: צופן c נסמן $c \leftarrow Enc(m,k)$ לפעמים נגביל את עצמנו להצפנה של הודעות באורך מסויים, כלומר נניח ש- $m \in \{0,1\}^{\ell(n)}$ עבור פונקציה כלשהי $\ell: \mathbb{N} \to \mathbb{N}$. כלומר גודל ההודעות שנצפין יכול להיות תלוי בפרמטר הבטיחות.
Dec	אלגוריתם פענוח (בדרך כלל דטרמניסטי) קלט: צופן c ומפתח k פלט: הודעה m יתכן כי $Dec(c,k)$ מחזיר $\perp$ שמשמעותו כי c לא הצפנה חוקית.

דרישת נכונות: לכל n, לכל k כל ש- $k \leftarrow Gen\ (1^n)$, ולכל $m \in \{0,1\}^*$ מתקיים
$Dec(Enc(m,k),k) = m$

אז עכשיו אנחנו צריכים להגדיר מהי מתקפה ומהו ניצחון. נתחיל מהמתקפה הפשוטה ביותר:

תסריט המתקפה הפשוט ביותר: היריב רואה הצפנה אחת בלבד וצריך **ללמוד מידע** על ההודעה שהוצפנה.

איך נפרמל "ללמוד מידע"?

עבור מערכת הצפנה במפתח סימטרי $\Pi = (Gen, Enc, Dec)$ ועבור יריב $\mathcal{A}$ נגדיר את המשחק $\mathrm{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi}(n)$ באופן הבא:

1. היריב $\mathcal{A}$ מופעל על קלט 1^n ובוחר זוג מסרים m_0, m_1 כך ש- $|m_0| = |m_1|$. היריב שולח את ההודעות למצפין.
2. המצפין מריץ $k \leftarrow Gen(1^n)$, בוחר ביט $b \in \{0,1\}$ באקראי, מחשב $c \leftarrow Enc(m_b,k)$ ושולח את c ליריב.
3. היריב (צריך לנחש את b) מחזיר ניחוש $\hat{b}$. היריב מנצח אם $\hat{b} = b$.

<u>הגדרה:</u> למערכת הצפנה במפתח סימטרי Π יש *הצפנות בלתי מובחנות מפני מאזין (EAV-בטוחה)* אם לכל יריב פולינומי אקראי $\mathcal{A}$ קיימת פונקציה זניחה $negl$ כך שלכל n מתקיים

$$\Pr\begin{bmatrix}\text{היריב } \mathcal{A} \text{ מנצח}\\ \text{במשחק } \mathrm{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi}(n)\end{bmatrix} \le \frac{1}{2} + negl(n)$$

כאשר ההסתברות היא מעל המטבעות האקראיים של $\mathcal{A}$, בחירת המפתח k, בחירת הביט b, והאקראיות של ההצפנה.

הערות:

1. המתקיף רק מאזין – לא רואה הצפנות אחרות ולא יכול לבקש הצפנה או פענוח של הודעות אחרות.
2. ההגבלה על היריב שההודעות m_0, m_1 הן מאותו האורך אומרת שאנחנו לא מגינים על אורך ההודעה המוצפנת.
3. עבור הודעות מתחום $m_0, m_1 \in \{0,1\}^{\ell(n)}$ ההגדרה כנ"ל.
4. אנחנו לא מניחים שום דבר על <u>האסטרטגיה</u> של היריב כשהוא מנסה להבחין בין 2 ההודעות. זאת נקודה חשובה. ההגדרה שלנו מבטיחה בטיחות כנגד <u>כל</u> יריב, לא משנה איך הוא פועל....

<u>דוגמה למערכת הצפנה בטוחה – One Time Pad (OTP)</u>

- יצירת מפתח: הגרל $k \in \{0,1\}^n$ בהתפלגות אחידה
- הצפנה של הודעה $m \in \{0,1\}^n$:

$$Enc(m,k) = m \oplus k$$

- פענוח של צופן $c \in \{0,1\}^n$:

$$Dec(c,k) = c \oplus k$$

משפט: מערכת ההצפנה OTP היא EAV-בטוחה

הוכחה:

$$\Pr[\text{מנצח } \mathcal{A}] = \sum_{m_0,m_1}\left(\Pr\begin{bmatrix}\text{היריב}\\ \text{מנצח}\end{bmatrix} \wedge \underset{m_0,m_1}{\text{היריב בוחר}} \wedge b = 0\right] + \Pr\begin{bmatrix}\text{היריב}\\ \text{מנצח}\end{bmatrix} \wedge \underset{m_0,m_1}{\text{היריב בוחר}} \wedge b = 1\right]\Bigg)$$

$$= \sum_{m_0,m_1}\left(\Pr\begin{bmatrix}\text{היריב}\\ \text{מנצח}\end{bmatrix} m_0,m_1 \wedge b = 0\Bigg] \cdot \Pr\begin{bmatrix}m_0,m_1\\ \wedge\, b = 0\end{bmatrix} + \Pr\begin{bmatrix}\text{היריב}\\ \text{מנצח}\end{bmatrix} m_0,m_1 \wedge b = 1\Bigg] \cdot \Pr\begin{bmatrix}m_0,m_1\\ \wedge\, b = 1\end{bmatrix}\right)$$

נשים לב שבחירת b היא בלתי תלויה בבחירת m_0, m_1 ולכן

$$\Pr[m_0, m_1 \wedge b = 0] = \Pr[b = 0\,] \cdot \Pr[m_0, m_1] = \frac{1}{2} \cdot \Pr[m_0, m_1]$$

וגם

$$\Pr[m_0, m_1 \wedge b = 1] = \Pr[b = 1\,] \cdot \Pr[m_0, m_1] = \frac{1}{2} \cdot \Pr[m_0, m_1]$$

ולכן

$$\Pr[\text{מנצח } \mathcal{A}] = \frac{1}{2}\sum_{m_0,m_1}\Pr\begin{bmatrix}\text{היריב}\\ \text{בוחר}\\ m_0,m_1\end{bmatrix}\cdot\left(\Pr\begin{bmatrix}\text{היריב}\\ \text{מנצח}\end{vmatrix} m_0,m_1\\ \wedge\, b=0\end{bmatrix}+\Pr\begin{bmatrix}\text{היריב}\\ \text{מנצח}\end{vmatrix} m_0,m_1\\ \wedge\, b=1\end{bmatrix}\right)$$

ננתח את הביטויי שבתוך הסוגריים. נראה שלכל m_0,m_1 מתקיים שהביטויי בתוך הסוגריים הוא 1:

$$\Pr\begin{bmatrix}\text{היריב}\\ \text{מנצח}\end{vmatrix} m_0,m_1\\ \wedge\, b=0\end{bmatrix}+\Pr\begin{bmatrix}\text{היריב}\\ \text{מנצח}\end{vmatrix} m_0,m_1\\ \wedge\, b=1\end{bmatrix}=\Pr\begin{bmatrix}\text{היריב}\\ \text{מחזיר}\\ 0\end{vmatrix} m_0,m_1\\ \wedge\, b=0\end{bmatrix}+\Pr\begin{bmatrix}\text{היריב}\\ \text{מחזיר}\\ 1\end{vmatrix} m_0,m_1\\ \wedge\, b=1\end{bmatrix}=$$

$$=\sum_c\left(\Pr\begin{bmatrix}\text{היריב} & & \text{הצופן}\\ \text{מחזיר} & \wedge & \text{הוא}\\ 0 & & c\end{vmatrix} m_0,m_1\\ \wedge\, b=0\end{bmatrix}+\Pr\begin{bmatrix}\text{היריב} & & \text{הצופן}\\ \text{מחזיר} & \wedge & \text{הוא}\\ 1 & & c\end{vmatrix} m_0,m_1\\ \wedge\, b=1\end{bmatrix}\right)$$

$$=\sum_c\left(\Pr\begin{bmatrix}\text{הצופן}\\ \text{הוא}\\ c\end{vmatrix} m_0,m_1\\ \wedge\, b=0\end{bmatrix}\cdot\Pr\begin{bmatrix}\text{היריב}\\ \text{מחזיר}\\ 0\end{vmatrix} m_0,m_1\\ b=0\\ c\end{bmatrix}+\Pr\begin{bmatrix}\text{הצופן}\\ \text{הוא}\\ c\end{vmatrix} m_0,m_1\\ \wedge\, b=1\end{bmatrix}\cdot\Pr\begin{bmatrix}\text{היריב}\\ \text{מחזיר}\\ 1\end{vmatrix} m_0,m_1\\ b=1\\ c\end{bmatrix}\right)$$

$$=\sum_c\left(\Pr[Enc(m_0,k)=c]\cdot\Pr\begin{bmatrix}\text{היריב}\\ \text{מחזיר}\\ 0\end{vmatrix} m_0,m_1\\ b=0\\ c\end{bmatrix}+\Pr[Enc(m_1,k)=c]\cdot\Pr\begin{bmatrix}\text{היריב}\\ \text{מחזיר}\\ 1\end{vmatrix} m_0,m_1\\ b=1\\ c\end{bmatrix}\right)$$

$$=\sum_c\left(\frac{1}{2^n}\cdot\Pr\begin{bmatrix}\text{היריב}\\ \text{מחזיר}\\ 0\end{vmatrix} m_0,m_1\\ b=0\\ c\end{bmatrix}+\frac{1}{2^n}\cdot\Pr\begin{bmatrix}\text{היריב}\\ \text{מחזיר}\\ 1\end{vmatrix} m_0,m_1\\ b=1\\ c\end{bmatrix}\right)$$

$$=\frac{1}{2^n}\cdot\sum_c\left(\Pr\begin{bmatrix}\text{היריב}\\ \text{מחזיר}\\ 0\end{vmatrix} m_0,m_1\\ b=0\\ c\end{bmatrix}+\Pr\begin{bmatrix}\text{היריב}\\ \text{מחזיר}\\ 1\end{vmatrix} m_0,m_1\\ b=1\\ c\end{bmatrix}\right)$$

$$\overset{*}{=}\frac{1}{2^n}\cdot\sum_c\left(\Pr\begin{bmatrix}\text{היריב}\\ \text{מחזיר}\\ 0\end{vmatrix} m_0,m_1\\ b=0\\ c\end{bmatrix}+\Pr\begin{bmatrix}\text{היריב}\\ \text{מחזיר}\\ 1\end{vmatrix} m_0,m_1\\ \boldsymbol{b=0}\\ c\end{bmatrix}\right)=\frac{1}{2^n}\cdot\sum_c 1=\frac{1}{2^n}\cdot 2^n=1$$

הסבר למעבר המסומן ב *: מכיוון שהיריב לא רואה את b אלא רק את m_0,m_1,c אז ההסתברות שיחזיר 0 בהינתן $m_0,m_1,b=0,c$ שווה להסתברות שיחזיר 0 בהינתן $m_0,m_1,b=1,c$ ולכן הסכום של 2 ההסתברויות האלה הוא 1.

נציב בחשבון הקודם שעשינו:

$$\Pr[\text{מנצח } \mathcal{A}] = \frac{1}{2}\sum_{m_0,m_1}\Pr\begin{bmatrix}\text{היריב}\\ \text{בוחר}\\ m_0,m_1\end{bmatrix}\cdot 1=\frac{1}{2}$$

מ.ש.ל.

הערות:

- ההסתברות של היריב לנצח במשחק היא בדיוק 1/2
- המערכת עמידה גם כנגד יריב שאינו מוגבל חישובית
- המערכת עמידה רק כנגד הצפנה של הודעה אחת
- הבעיות עם מערכת ההצפנה OTP הן:
  - אורך המפתח שווה לאורך ההודעה
  - אפשר להשתמש במערכת רק פעם אחת! נרצה מערכת שאפשר להשתמש בה הרבה פעמים.