יסודות הקריפטוגרפיה שיעור 1#

הקדמה:

- אתר הקורס: http://tau-crypto.wikido.com
- שיעורי בית יפורסמו באתר (כבר פורסמו).
- המרצה: בני שור. המתרגל: רני הוד.
- ציונים: 70-80% בחינה, 20-30% תרגילי הבית, למעבר הקורס חייבים לעבור את הבחינה.
- לבחינה ניתן להכניס שני עמודים דו צדדיים
- יהיו 4-5 תרגילי בית (*Sage/Maple/Wolfram Alpha program*).
- תקשורת: benny@tau.ac.il.

הגדרות וסימונים:

- פונקציית *encryption*: E
- פונקציית *Decryption*: D
- מפתח *encryption*: k_1
- מפתח *decryption*: k_2
- מרחב ההודעות: M, בד"כ k מאותו אורך הודעה.
- דרישת קונסיסטנטיות: $\forall m \in M, matching\ k_1, k_2 : D_{k_2}\left(E_{k_1}(m)\right) = m$

מודל תקשורת: שני צדדים (אליס ובוב), מניחים כי לשניהם את אותו אלגוריתם פענוח והצפנה ואת אותם מפתחות

מטרות מערכת אבטחה:

- אף יריב לא יוכל לגלות מהי m.
- אף יריב לא יוכל להקיש שום אינפורמציה בעלת משמעות מההודעה

שאלות חשובות:

- מה היריב יודע לפני?
- מהם המשאבים החישוביים שיש בידי היריב? לרוב נניח כי היריב מוגבל **פולינומית**.

צד שלישי: חוה (*Eve*), המכירה את האלגוריתמים E,D, את מרחב ההודעה M, ורוצה לגלות את m. כמו כן מניחים כי היא שמעה את ההצפנה, כלומר את $E_{k_1}(m)$. היא **אינה יודעת** את k_1, k_2.

Plaintext – ההודעה לפני ההצפנה; *Ciphertext* – אחרי ההצפנה; *symmetric cryptosystem* – מערכת הצפנה סימטרית בה $k_1 = k_2$.

דוגמאות:

- *Shift cipher*: הזזת התוים במרחק קבוע. למשל "בית" יעבור בהזזה ב-1 ל-"גכא". חסרון: מרחב המפתחות קטן מדי.
- *Substitution Cipher*: צופן הצבה; פרמוטציה של האותיות, למשל א' יעבור ל-ג', ב' יעבור ל-ת' וכן הלאה. באנגלית נקבל $26! \cong 4 \cdot 10^{27}$ מפתחות אפשריים. מעבר על כל התמורות לא יעבוד כי יש יותר מדי. אבל, מרחב גדול הוא תנאי הכרחי אך לא מספיק לבטיחות.

ניתן לנסות לפענח את הקידוד ע"י בדיקת סדר השכיחות של האותיות בהודעה המוצפנת, ולהשוות לשכיחות האותיות במילים בשפה האנגלית. עם טקסט מוצפן (*ciphertext*) מספיק ארוך, סביר שניתן יהיה לפענח. ניתן להתבסס גם על סטטיסטיקות של זוגות אותיות במילים בשפה האנגלית (בפועל מסתבר שעל סמך אותיות בודדות קשה לפענח).

***Perfect Cipher*: הצפנה מושלמת**

מרחב ההודעות הלא מוצפנות הוא $\{0,1\}^n$. הנחה: פילוג ההודעות אינו אחיד.

בהינתן טקסט מוצפן C, הסיכוי ש-$M = D_{k_2}(C)$ לכל M (מרחב הודעות לא מוצפנות) שווה להתפלגות האפריורית ש-M הוא מרחב ההודעות הלא מוצפנות. כלומר רוצים ש-M הנ"ל תתפלג באופן זהה לפילוג של הודעות מקוריות

<u>דוגמא</u>: אם ההודעות המקוריות 0 ... 000 בהתפלגות 0.5, וגם 1 ... 111 בהתפלגות 0.5, אז גם ההודעות המוצפנות יהיו בהתפלגות זו.

$$\Pr[plaintext = P|C] = \Pr[plaintext = P]$$

אם ההתפלגות לא זהה, אז מקבלים איזושהי אינפורמציה על ההודעה. מערכת כזו ניתנת לבניה בקלות אך בעלות גבוהה.

הערה: אין להניח שפילוג ההודעות אחיד.

<u>דוגמא</u>: *One time pad*

$M = \{0,1\}^n$ (מרחב ההודעות), $\{0,1\}^n$ הוא גם מרחב המפתחות. המפתח k נבחר באופן רנדומאלי ובלתי תלוי ב-P. XOR הוא אלגי' הצפנה סימטרי:

$$E_k(P) = C = P \oplus k, \;\; D_k(C) = C \oplus k = P$$

כש-k נבחר אקראית ב-$\{0,1\}^n$, גם C מתפלג אחיד על $\{0,1\}^n$ בלי תלות ב-P. אמנם זוהי הצפנה מושלמת, אך גודל המפתח כגודל ההודעה – גדול מאוד.

Theorem (Claud Shannon): בהינתן *perfect cipher*, גודל מרחב המפתחות הוא כגודל מרחב ההודעות.

Vigenere Cipher:

<u>דוגמא</u>: המפתח הסודי הוא *beads*. שמים את המפתח בחזרות רציפות תחת ההודעה, והמספר שמייצג כל תו במפתח (2 ל-b וכן הלאה) מסמל הזזה של האות המתאימה במיקום זה בהודעה המקורית.

אם גודל המפתח הוא 1, קיבלנו אלגוריתם הזזה; אם הוא 2, נקבל הזזה של זוגיים במרחק קבוע ואי זוגיים במרחק קבוע. אם $k = l$, זהו *one-time pad* (כאשר l אורך ההודעה, במקרה של הודעה בביטים ולא בשפה האנגלית).

משאבים חישוביים:

האינפורמציה לרוב קיימת אך שבירת הפענוח לוקחת משאבי זמן שאינם זמינים בפועל 2^{70} צעדים הם ברי ביצוע, 2^{100} לא.

התקפות אפשריות:

- האזנה.
- הודעות ידועות: הקשה ממידע חיצוני (למשל) על פענוח הודעה מוצפנת שבידי היריב
- ועוד כל מיני.

סימונים מועילים: (פרק ראשון ב-*Stinson*)

- $a \equiv b (mod\ m)$: m מחלק את $a - b$.
- $a\ mod\ b$ (ללא סוגריים): מסמן את השארית של a בחלוקה ב-b (מספר בין 0 ל-$b-1$). למשל: $2 = 3\ mod\ 5$.
- החוג ($ring$) $\mathbb{Z}_m$: פעולות אריתמטיות מודולו m. פורמלית: $(\mathbb{Z}_m, +, \cdot)$ כאשר $+, \cdot$ הם סימונים לחיבור וכפל מודולו m והאיברים הם $\{0,1,\dots,m-1\}$. תכונות החוג:
  - סגירות תחת חיבור וכפל: $a,b \in \mathbb{Z}_m \Rightarrow a+b \in \mathbb{Z}_m, \;\; a \cdot b \in \mathbb{Z}_m$.
  - קומוטטיביות ואסוציטיביות חיבור וכפל.
  - דיסטריביוטיביות: $a \cdot (b+c) = a \cdot b + a \cdot c$.
  - איבר נטרלי לחיבור: 0; איבר ניטרלי לכפל: 1.
  - אם $a \in \mathbb{Z}_m$ אז $b \in \mathbb{Z}_m$ הוא <u>הופכי כפלי</u> שלו אם $a \cdot b = 1$. ל-0 אין הופכי כפלי, ול-1 יש: 1. לא לכל איבר בחוג יש הופכי כפלי (למשל ב-$\mathbb{Z}_6$ ו-$a = 2$: ל-2 אין הופכי כפלי, מניסיון עבור כל $b \in \mathbb{Z}_6$).

<u>השערה</u>: אם $a\ \nmid m$ (a לא מחלק את m), אז ל-a יש הפכי כפלי: לא נכון, ע"י דוגמא נגדית.

טענה: (כרגע ללא הוכחה)

אם $\gcd(a,m) = 1$ (המחלק המשותף המקסימלי הוא 1) אז ל-a יש הפכי כפלי ב-$\mathbb{Z}_m$.