יסודות הקריפטוגרפיה שיעור 2#

הקדמה מתמטית (מצגת *2b*):

נלמד כל מיני משפטים שאין צורך לדעת את ההוכחה שלהם, לא נשאל על שום הוכחה שלא תיעשה בכיתה.

אקסיומות חבורה חילופית - *Groups*:

חבורה: קבוצה G לא ריקה סופית/אינסופית של איברים ופעולה + (סימון) על זוגות של איברים. מתקיים:

- סגירות תחת +: $a+b \in G$
- אסוציטיביות: $(a+b)+c = a+(b+c)$
- קומוטטיביות: $a+b = b+a$
- קיים איבר ניטרלי 0: $a+0 = a$
- קיום הופכי: $a+b_a = 0$

דוגמא: $(\mathbb{Z},+)$ כאשר + הוא חיבור רגיל.

חבורות לא קומוטטיביות יסומנו: הפעולה תסומן כמו כפל ($\cdot$) והאיבר הניטרלי יסומן 1. למשל חבורת המטריצות (כפל מטריצות לא קומוטטיבי).

תתי חבורות: $(H,+)$ תת חבורה של $(G,+)$ אם היא חבורה ו-$H \subseteq G$.

דוגמא: עבור $(\mathbb{Z},+)$, $(\mathbb{N},+)$ אינה חבורה כי אין הופכי. אבל הזוגיים: $(\mathbb{Z}_{even},+)$ הם כן תת חבורה.

טענה: אם $(G,+)$ חבורה **סופית**, $H \subseteq G$ ו-H סגורה לחיבור, אז $(H,+)$ חבורה בעצמה. הדוגמא עם $\mathbb{Z},\mathbb{N}$ היא מדוע צריך חבורה סופית.

משפט *Lagrange*:

אם $(G,+)$ היא חבורה סופית ו-$(H,+)$ (עם אותה פעולה +) היא תת-חבורה שלה אז $|H|$ מחלקת את $|G|$.

דוגמא: $(\mathbb{Z}_{12},+_{12})$ (חיבור מודולו 12); החבורה $(\{0,3,6,9\},+_{12})$ היא תת חבורה שלה ויש בה 4 איברים ואכן 4 מחלק את 12.

סימון: $a^n := \underbrace{a+a+\cdots+a}_{n\ times}$

סדר: נאמר כי a מסדר n אם $a^n = 0$ אבל לכל $m < n$ מתקיים $a^m \neq 0$.

דוגמא: ב-$\mathbb{Z}_{12}$ עם חיבור מודולו 12, הסדר של 4 הוא 3; הסדר של 5 הוא 12; הסדר של 1 הוא גם 12; כנ"ל 7 ו-11 (כל הזרים ל-12).

טענה: בחבורה סופית, לכל a יש n שהוא לכל היותר סדר החבורה כך ש-$a^n = 0$ (הסדר של a הוא n).

הוכחה: אם נסתכל על הסדרה $a, a^2, a^3, \dots$, אז בסדרה זו חייבת להיות חזרה כיוון ש-G סופית, כלומר קיימים n_1, n_2 (שונים זה מזה) כך ש-$a^{n_1} = a^{n_2}$ (בה"כ $n_1 < n_2$), אז נקבל $0 = a^{n_1} - a^{n_1} = a^{n_2} - a^{n_1} = a^{n_2-n_1} = a^l$, כאשר l הוא הסדר של a.

חבורה ציקלית:

טענה: נניח G היא חבורה **סופית**, ו-a איבר מסדר n, אזי $< a > := \{0, a, \dots, a^{n-1}\}$ היא תת חבורה של G.

הוכחה: איברים בקבוצה הם מהצורה a^l, a^k. מתקיים ש-$a^l + a^k = a^{l+k}$. אם $l+k < n$ אז הסכום בקבוצה, ואם לא אז $a^{l+k} = a^{l+k-n}$, וגם הוא בקבוצה.

[*** הערה: צריך לשים לב לסימון +, שלעתים יציין פעולת חבורה ולעתים פעולת החיבור הרגילה]

$< a >$ נקראת תת חבורה ציקלית שנוצרת ע"י a, ו-a הוא היוצר של החבורה. לפי משפט *Lagrange*, n מחלק את גודל G.

משפט *Fermat* הקטן:

יהי p מספר ראשוני, אז לכל $a \in \{1, \dots, p-1\}$ מתקיים: $a^{p-1} \bmod p = 1$, כאשר החזקה כאן משמעותה העלאה בחזקה ולא פעולת החיבור $p-1$ פעמים כפי שהוגדרה לעיל. נשים לב כי 0 לא איבר בקבוצה.

הוכחה:

כדי להוכיח את המשפט נעבוד בחבורה "חדשה" – $(\mathbb{Z}_p^*,\cdot_p)$, כאשר $\cdot$ היא פעולת הכפל מודולו p ו-$\mathbb{Z}_p^*$ הוא כמו $\mathbb{Z}_p$ רק בלי האיבר 0. למשל $(\mathbb{Z}_7,\cdot_7)$ מתקיים: $6 \cdot_7 5 = 2$ (כי $30 \bmod 7 = 2$). קבוצה זו היא חבורה (יוכח בהמשך).

אם כן, בחבורה $(\mathbb{Z}_p^*,\cdot_p)$ יש $p-1$ איברים. הסדר של כל איבר a בחבורה זו מחלק את $p-1$. הסדר של a הוא n פרושו כאן ש-$a^n \bmod p = 1$. לפי משפט *Lagrange*, $n|p-1$ כאשר $p-1$ סדר החבורה. כלומר, קיים m טבעי כך ש-$n \cdot m = p-1$ (כפל של הטבעיים). מכאן:

$$(a^n)^m \bmod p = 1 \Rightarrow [a^{n\cdot m} = a^{p-1}] \Rightarrow a^{p-1} \bmod p = 1$$

משפט: לכל p ראשוני החבורה $\mathbb{Z}_p^*$ היא ציקלית.

חוגים – *Rings*:

<u>חוג</u>: קבוצה לא ריקה R עם 2 פעולות $+$ ו-$\cdot$. תכונות:

- תכונות ביחס ל-$+$ כמו בחבורה.
- קומוטטיביות גם ביחס לכפל.
- קיום איבר ניטרלי גם ביחס לכפל.
- לא נדרש הופכי ביחס לכפל.
- רשימת תכונות מלאה במצגת *2b*.

בד"כ $1 \neq 0$ (סימונים לניטרליים ביחס ל"חיבור" ול"כפל").

דוגמא: חוג קומוטטיבי עם יחידה (כפלית): $(\mathbb{Z}_m, +, \cdot)$ (פעולות מודולו m). אם m לא ראשוני אז בחוג זה יש איברים רבים שאינם 0 ללא הופכי כפלי. גם $\mathbb{Z}$ הוא חוג ללא הופכיים כפליים פרט ל-$1\pm$.

שדות:

<u>שדות</u>: קבוצה לא ריקה F עם פעולות $+, \cdot$ שהיא למעשה חוג בו לכל איבר שונה מ-0 יש הופכי כפלי.

דוגמא: $\mathbb{Z}_p$ כאשר p ראשוני, $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.

תכונות מעל שדות:

יהי $f(x) = a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + \cdots + a_1 x + a_0$ פולינום מדרגה n מעל שדה F.

משפט: למשוואה $f(x) = 0$ יש לכל היותר n פתרונות ב-F (שורשים ל-$f(x)$).

דוגמא: כמה שורשים יש ל-$x^3 + 17x + 3$ מעל $\mathbb{Z}_{19}$? לכל היותר 3.

<u>הערה</u>: המשפט לא חל על חוג עם זהות, למשל ב-$\mathbb{Z}_{24}$ למשוואה $6x = 0$ יש 6 שורשים $(0,4,8,12,16,20)$.

שאריות פולינומים:

במספרים טבעיים פעולת השארית היא פעולה בסיסית והיא מועילה מאוד בחישובי gcd. למשל: $31 \ mod \ 7 = 3$ והשארית קטנה מהמחלק.

משפט:

יהיו $f(x)$ מדרגה n, $g(x)$ מדרגה m כאשר $n \geq m$, אז קיים פולינום $r(x)$ מדרגה <u>קטנה</u> מ-m ופולינום ייחודי נוסף $h(x)$, שניהם מעל F, כך ש-$f(x) = h(x) \cdot g(x) + r(x)$. הפולינום $r(x)$ מכונה <u>השארית</u> של $f(x)$ מודולו $g(x)$. השארית היא 0 אם $g(x) | f(x)$.

<u>שדה סופי</u>: שדה בו F היא קבוצה סופית.

מתברר כי לכל p ראשוני מתקיים ש-$(\mathbb{Z}_p, +, \cdot)$ הוא <u>שדה סופי</u>.

שאלה: לאיזה m טבעי $\mathbb{Z}_m$ הוא שדה סופי? ב-$\mathbb{Z}_{26}$ ל-13 ול-2 אין הופכי כפלי. יש עוד, בהמשך.

<u>מציין של שדה סופי (*Characteristic*)</u>: ה-n המינימלי הטבעי כך ש-$\underbrace{1+1+..+1}_{n \ times} = 0$. סימון: $char(F)$.

משפט: $char(F)$ הוא תמיד ראשוני.

<u>שדות גלואה</u>: $GF(p^k)$:

לכל חזקת מספר p ראשוני p^k $(k = 1,2,3 ...)$, קיים שדה סופי עם p^k איברים המקיים. סימון $F = GF(p^k)$. תכונות:

- $char(F) = p$
- $GF(p^k)$ ו-$\mathbb{Z}_{p^k}$ אינם אותו דבר!

עד כאן הקדמה מתמטית, המשך יבוא.

Pseudo Random Generator:

יוצר של מספרים פסאודו אקראיים מתחיל מ-*truly random seed* של n ביטים אקראיים ומעביר דרך PRG ל-m ביטים $(m > n - pseudo\ random$ *string* שאמור "להראות אקראי" מול *distinguisher* - מבחין מוגבל. בעצם מרחיבים את האקראיות מגרעין אקראי בעל n ביטים למחרוזת רחבה "משמרת אקראיות".

<u>הגדרה</u>: PRG בטוח חישובית (שימו לב שללא מגבלות חישוביות, שום PRG לא יהיה בטוח). התוכנית PRG עצמה צריכה להיות פולינומיאלית, ומרחיבה את הקלט כך ש-$m = n^c, c > 1$. כמו כן PRG צריכה להיות דטרמניסטית (לא ה-$seed$ שלה).

נניח שהיריב, נסמנו D (מלשון $distinguisher$, מבחין) רץ בזמן פולינומיאלי באורך הקלט, m, מותר לו להטיל מטבעות והוא מכיר את PRG.

היריב D מקבל כקלט מחרוזת באורך m ומוציא פלט "כן"/"לא".

- $PRG(r) \xrightarrow[r\in\{0,1\}^n]{} \boxed{D} \to \begin{cases} y \\ n \end{cases}$: $p_1 = \Pr[D\ says\ Yes]$, הסתברות על כל r ועל הטלות D.
- $s \xrightarrow[s\in\{0,1\}^m]{} \boxed{D} \to \begin{cases} y \\ n \end{cases}$: $p_2 = \Pr[D\ says\ Yes]$, הסתברות על כל $s \in \{0,1\}^m$ ועל הטלות D.

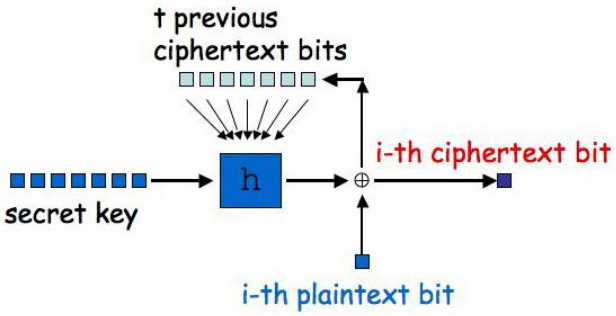
נאמר כי PRG חזק אם לכל D כנ"ל זניח $> |p_1 - p_2|$ (קטן מכל פולינום כש-$n \to \infty$).

Synchronous Stream Ciphers :

לשני הצדדים יש $seed$ משותף של $pseudo\ random\ gen$. רוצים להשתמש בו כדי לייצר מחרוזת ארוכה ובה להשתמש ב-$one\ time\ pad$ (ראינו שיעור שעבר, שימוש ב-xor). נניח המצפין מכניס את ה-$seed$ ל-PRG, מייצר מחרוזת, ואיתה עושה xor עם הטקסט שלו ומייצר $ciphertext$. הצד המפענח משתמש ב-$seed$ שברשותו וב-PRG כדי לעשות xor ל-$ciphertext$ עם המחרוזת $PRG(seed)$ ולקבל חזרה את ה-$plaintext$.

חסרון המערכת: שני הצדדים צריכים להחזיק ב-$seed$.

Asynchronous Stream Ciphers :



מתחילים מ-$seed$, ומייצרים $ciphertext$, ו-t הביטים האחרונים ש ל הפלט של ה-$ciphertext$ נכנס כקלט, המשך ל-$secret\ key$.

פענוח לדוגמא: $c_{100}, \dots, c_{200}$ הלכו לאיבוד. החל מ-c_{201} התקשורת חזרה, מתחילים למלא את ה-$buffer$ וכשיהיו שם $c_{201}, \dots, c_{210}$ ניתן להמשיך לפענח.

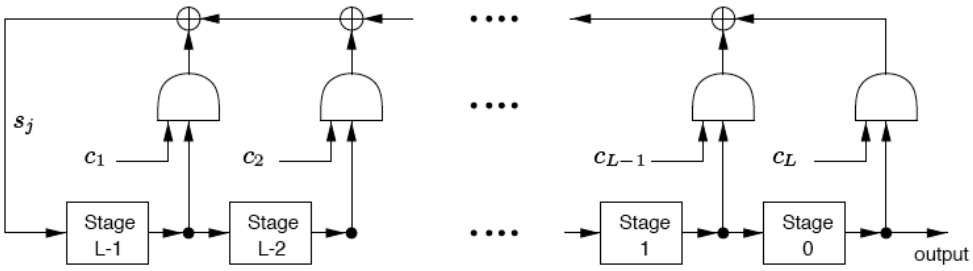
קודם נלקח ה-$seed$ והורחב בפעם אחת, ופה גם – רק שההרחבה נבנית צעד צעד עם התקדמות ההצפנה.

סינכרוני לעומת א-סינכרוני: מפורט במצגת.

Real Synchronous Stream Ciphers : מפורט במצגת.

<u>*LFSR – linear feedback shift registers*</u> :

מייצר זרם פלט בינארי. c_i הם קבועים. מערכות אלו מהירות אבל לא בטוחות. ה-$seed$ הוא כל ה-c_i. עם מספיק ביטים ניתן לפענח את ה-$seed$.



<u>דוגמא - *RC4*</u> : במצגת.