יסודות הקריפטוגרפיה תרגול #3

<u>המציין של שדה סופי</u>: מספר הפעמים שצריך לחבר 1 לעצמו כדי לקבל 0. המציין הזה תמיד ראשוני לכל שדה סופי.

המציין של $GF(p^k)$ הוא p. $GF(p) = \mathbb{Z}_p$, פעולות כפל וחיבור מודולו p.

<u>$GF(p^k)$</u>: נסמן את החבורה הכפלית של שדה F ב-F^*. נסמן $F = GF(p^k)$, אז F^* בעל $q := p^k - 1$ איברים.

משפט לגרנג': לכל $a \in F^*$ הסדר של a, נסמנו n מחלק את q: $n|q$.

נניח ש-$ord_{F^*}(a) = l$, וגם $a^j = 1$. לא יתכן $j < l$ כי אז l לא מינימלי. נסתכל על $j \bmod l$:

$$1 = a^j = a^{j \bmod l} \Rightarrow j \bmod l = 0 \Rightarrow l|j$$

Primitive elements in $GF^*(p^k)$:

טענה: F^* היא חבורה ציקלית, כלומר קיים $g \in F^*$ כך ש- $\left\{g, g^2, .., g^{p^k-1}\right\}_{=1} = F^*$ (הסימון כמו לעיל $F^* = GF^*(p^k)$). איבר g זה נקרא איבר פרימיטיבי של F^*. טענה זו לא נכונה בשדות אינסופיים כמו $\mathbb{R}, \mathbb{C}, \mathbb{Q}$.

אריתמטיקה של פולינומים:

יש לא מעט אנלוגיות בין מספרים טבעיים ובין פולינומים:

א. <u>גודל</u> (מס' ביטים בטבעיים, דרגה בפולינומים).

ב. <u>שאריות</u>: נניח $f(x), g(x)$ ($\deg(f) \geq \deg(g)$) שני פולינומים מעל שדה. קיימים שני פולינומים $h(x), r(x)$ יחידים כך ש- $f(x) = h(x) \cdot g(x) + r(x)$ ו-$\deg(r) < \deg(g)$; במספרים: $F = H \cdot G + R$ (עבור מספרים).

ג. <u>*GCD*</u>: מוגדר על פולינומים ועל מספרים.

ד. <u>ראשוניות</u>: מספר ראשוני לעומת פולינום אי פריק. מהצד השני: פירוק לגורמים.

נניח כי $f(x)$ פולינום אי פריק מדרגה k מעל $GF(p^k)$. שדה זה ניתן לייצוג ע"י פולינומים מדרגה $k-1$ (או פחות) מעל $GF(p)$ (יש p^k כאלה – k מקדמים ו-p אפשרויות לכל מקדם).

אם f פולינום מדרגה k ו-g, h פולינומים מדרגה $k-1$, להכפלתם: $g \cdot h \bmod f$ - מתקבל פולינום מדרגה $k-1$ (חישוב שארית לפולינום מדרגה $2k-2$ ביחס לפולינום מדרגה k יתן $2k-2-(k-1) = k-1$).