

שיעור 4 מבוא לקריפטוגרפיה מודרנית

23 בנובמבר 2016

הגדרה 0.1 פונקציית ϕ של אוילר

נתון $1 \leq m$ טבעי, כמה מספרים טבעיים $\mathbb{Z}_m$ $(0 \leq a \leq m-1)$, הם זרים ל- m ($\gcd(m, a) = 1$). מספר הא-ים האלה מסומן על ידי $\phi(m)$. (Euler totient function).

הערה 0.2 אם m ו- n זרים, אזי מתקיים $\phi(m) \cdot \phi(n) = \phi(m \cdot n)$

הערה 0.3 אם $m = p^e$ ו- $e \geq 1$, p ראשוני, אזי $\phi(p^e) = p^e - p^{e-1}$

מסקנה 0.4 אם $m = p_1^{e_1} p_2^{e_2} \dots p_n^{e_n}$, אזי מתקיים:

$$\phi(m) = \phi(p_1^{e_1}) \cdot \phi(p_2^{e_2}) \cdot \dots \cdot \phi(p_n^{e_n}) = \prod_{i=1}^n (p_i^{e_i} - p_i^{e_i-1})$$

לדוגמא:

$$\phi(6) = \phi(3) \cdot \phi(2) = 2$$

$$\phi(12) = \phi(2^2) \cdot \phi(3) = 2 \cdot 2 = 4$$

$$\phi(p \cdot q) = (p-1)(q-1) \text{ מתקיים } p \neq q \text{ ראשוניים}$$

הערה 0.5 סיבוכיות אלגוריתם Euclid $\gcd$:

כמה שלבים מתבצעים באלגוריתם.

נניח ש- r_0 הוא בן n ביטים, כלומר $2^{n-1} \leq r_0 \leq 2^n - 1$, כמה שלבים יתבצעו במקרה הגרוע כפונקציה של n .

$$r_0 = c_0 r_1 + r_2 \text{ אחד: } r_0 = c_0 r_1 + r_2$$

טענה 0.6 $c_0 \geq 1$ (מאחר ו- $c_0 = 0$ היינו מקבלים $r_0 = r_2$ סתירה לכך ש- $r_0 > r_1 > r_2$)

ולכן $r_0 > r_1 + r_2 > 2r_2$ כלומר $r_2 < r_0/2$ הוא בן לכל היותר $n-1$ ביטים.

מסקנה 0.7 כל שתי איטרציות כמות הביטים יורדת בלפחות 1, מכאן אלגוריתם אוקלידס יסתיים בעד $2n$ צעדים.

1 ההמשך במצגת

- שדות סופיים והמאפיינים שלהם

- חבורות ציקלית

- חוגים (למשל $(\mathbb{Z}_m, +_m, \cdot_m)$), חוג עם יחידה, או הזוגיים הם חוג ללא יחידה)

- שדות/שדות סופיים

משפט 1.1 מעל כל שדה, לפולינום מדרגה n יש לכל היותר n שורשים.

טענה 1.2 לכל p ראשוני ו- $k \geq 1$ יש שדה סופי יחיד בן p^k איברים. (והוא לא $\mathbb{Z}_{p^k}$)

- מציין של שדה (ה- n המינימלי שמקיים $\overbrace{1_F + 1_F + \dots + 1_F}^n = 0_F$)

- שדות גלוואה

הערה 1.3 שדה F עם p^k מקיים $\text{char}(F) = p$

- שארית של חילוק פולינומים

- Sage

- מימוש האריתמטיקה של $GF(p^k)$ (שדות גלוואה)

יהי פולינום לא פריק $f(x)$ מדרגה k מעל $GF(p)$
 כמה פולינום מדרגה לכל היותר $k - 1$ מעל $GF(p)$ יש? (p^k)
 כל פולינום כזה מודולו $f(x)$ הינו איבר בשדה.
 פעולות השדה:
 חיבור: חיבור רגיל של פולינומים מעל $\mathbb{Z}_p$ מודולו .
 כפל: כפל פולינומים רגיל, ואז מודולו $f(x)$.

משפט 1.4 ניתן ללבנות מפסאודו רנדום גנרייטור פונקציית פסאודו אקראית, נראה את הבנייה:
 נניח יש לנו יוצר שמכפיל מחרוזות, $(n$ ביטים ל- $2n$ ביטים).
 מתחילים ממחרזת אקראית באורך n ביטים, מרחיב אותה למחרוזת בגודל $2n$,
 כעת נרחיב כל חצי (באורך n), בנפרד, וכך הלאה.
 עבור פונקציית אקראית $f : \{0, 1\}^l \rightarrow \{0, 1\}^n$, נעשה את הבנייה הזאת l פעמים.
 בפועל אי אפשר לבנות את העץ המלא, אבל בהינתן קלט ספציפי באורך l , ניתן לבנות את הפלט המתאים, (למשל 0 אומר התפצל ימינה ו1 התפצל שמאלה).
 GMV הוכיחו כי אם היוצר (בגודל n), אכן אקראי אזי הפונקציית אכן פסאודו אקראית.

- פרמוטציות פסאודו אקראיות
- הצפנות בלוקים
- איך לא נשלח כל פעם אותו מוצפן על אותה הודעה ? (Salting, stating)
- CBC
- OFB