

משך המבחן – שלוש שעות. השימוש במחשבון מותר. מרצה – דר' ארז שיינר

כל שאלה שווה 28 נקודות, כל ציון מעל 100 יעוגל ל-100.

1. תהי G חבורה סופית.

א. יהיו $h, g \in G$ איברים מסדר $o(h) = o(g) = 2$, הוכיחו/הפריכו: $o(gh) \leq 2$.

הפרכה: נביט ב- $(1\ 2), (1\ 3) \in S_3$.

מתקיים כי $o((1\ 2)) = o((1\ 3)) = 2$, אך $o((1\ 2)(1\ 3)) = o((1\ 3\ 2)) = 3$.

ב. יהי $g \in G$ איבר מסדר $o(g) = 113$. נסמן $h = g^3$ מצאו את $o(h)$.

נסמן $o(h) = t$ לכן $e = h^t = g^{3t}$. ראשית נראה כי $3t$ מתחלק ב-113 ללא שארית:

נחלק את $3t$ ב-113 ונקבל כי $3t = 113k + m$, כאשר $m < 113$.

$$e = g^{3t} = g^{113k+m} = (g^{113})^k g^m = e^k g^m = g^m$$

כיוון ש- $m < 113$ נובע כי $m = 0$.

כעת $3t = 113k$, כיוון ש-3 ראשוני ולא מחלק את 113 נובע ש- $k = 3a$.

לכן $t = 113a$, ולכן המספר החיובי הקטן ביותר ש- t יכול להיות הוא 113.

אכן, $h^{113} = (g^{113})^3 = e$ ולכן $o(h) = 113$.

2. תהי S_n חבורת התמורות מקבוצה בגודל n לעצמה, ותהי $G \subseteq S_n$ תת חבורה.

א. האם ייתכן ש $(1\ 3) \in G, (1\ 2) \in G$ אך $(1\ 3\ 2) \notin G$? הוכיחו קביעתכם.

כיוון ש $(1\ 3\ 2) = (1\ 3)(1\ 2) \in G$ מתוך סגירות בהכרח $(1\ 3\ 2) \in G$

ב. נניח כי G מכילה את כל התמורות האי זוגיות (מסימן שלילי) של S_n , הוכיחו כי $G = S_n$.

ראינו בהרצאה שכל תמורה ניתן להציג כהרכבה של מחזורים, וכל מחזור ניתן להציג כהרכבה של חילופים.

כיוון שחילוף הוא אי זוגי, G מכילה את כל החילופים.

בדומה לסעיף א', מתוך סגירות נובע כי כל התמורות שייכות ל G ולכן סה"כ $G = S_n$.

3. בוב רוצה לשלוח לאליס מסר מוצפן בשיטת RSA.

אליס מצאה ראשוני בטוח, כלומר ראשוני מהצורה $p = 2q + 1$ כאשר q ראשוני.

אליס נעזרה (בטעות) בראשוניים p, q ובנתה את המפתח הציבורי $n = pq = 34453$ ו $e = 7569$.

בוב שלח לאליס את המידע המוצפן $24847 = x^{7569} \pmod{34453}$

א. חשבו את הפרמטר הסודי $m = \phi(n)$. מדוע יכולתם לעשות זאת?

נתון כי $n = pq = (1 + 2q)q = 2q^2 + q$ לכן $2q^2 + q - 34453 = 0$

לכן $q = \frac{-1 \pm \sqrt{1 + 4 \cdot 2 \cdot 34453}}{2 \cdot 2} = \frac{-1 \pm 525}{4}$ כיוון ש q שלם (וחיובי) נובע כי $q = 131$.

סה"כ מצאנו כי $n = 263 \cdot 131$ ולכן $m = 262 \cdot 130 = 34060$

יכולנו לעשות זאת כיוון שאליס בחרה את המספרים הראשוניים בצורה שניתן למצוא אותם על ידי פתרון משוואה

ריבועית.

ב. מהו המידע x שבו שלח לאליס?

ראשית נחשב את $d = e^{-1} \pmod{m}$

$$\begin{aligned} \gcd(e, m) &= \gcd(34060, 7569) = \\ &= \gcd(34060 - 4 \cdot 7569, 7569) = \gcd(3784, 7569) = \\ &= \gcd(3784, 7569 - 2 \cdot 3784) = \gcd(3784, 1) = 1 \end{aligned}$$

לכן

$$\begin{aligned} 1 &= 1 \cdot 1 + 0 \cdot 3784 = 1 \cdot (7569 - 2 \cdot 3784) + 0 \cdot 3784 = \\ &= 1 \cdot 7596 - 2 \cdot 3784 = 1 \cdot 7596 - 2 \cdot (34060 - 4 \cdot 7569) = 9 \cdot 7569 - 2 \cdot 34060 \end{aligned}$$

לכן $d = 9$

לכן המידע שבו שלח הוא $x = 24847^9 \pmod{34453}$.

$$24847^2 \equiv 617373409 \equiv 10102 \pmod{34453}$$

$$24847^4 \equiv 10102^2 \equiv 102050404 \equiv 618 \pmod{34453}$$

$$24847^8 \equiv 618^2 \equiv 381924 \equiv 2941 \pmod{34453}$$

$$24847^9 \equiv 2941 \cdot 24847 \equiv 73075027 \equiv 214 \pmod{34453}$$

כלומר סה"כ $x = 214$

4. נביט בפולינום $g(x) = x^5 + x + 1$, המגדיר קוד פולינומי.

נסמן את המרחק המינימלי בין שתי מילים חוקיות ב d_{\min} .

א. קודדו את המידע 1011 באמצעות הקוד הפולינומי.

נקודד את הפולינום המתאים $f = x^3 + x + 1$.

ראשית נחלק את $x^5 f = x^8 + x^6 + x^5$ בפולינום $g(x) = x^5 + x + 1$ ונקבל שארית $r = x^4 + x^3 + x^2 + 1$.

לכן המילה המקודדת הינה $x^5 f + r = x^8 + x^6 + x^5 + x^4 + x^3 + x^2 + 1$

כלומר 101111101

ב. קבעו לגבי כל אחת מהמילים הבאות האם היא חוקית:

1100101, 1000111

נבדוק האם הפולינומים המתאימים $f = x^6 + x^5 + x^2 + 1$, $t = x^6 + x^2 + x + 1$ מתחלקים ב g ללא שארית.

אכן הפולינום $f = x^6 + x^5 + x^2 + 1$ מתחלק ב $g(x) = x^5 + x + 1$ ללא שארית, ולכן מדובר במילה חוקית.

לעומת זאת, כאשר מחלקים את $t = x^6 + x^2 + x + 1$ ב $g(x) = x^5 + x + 1$ נקבל שארית 1, כלומר מדובר במילה שאינה חוקית.

נשים לב (בשביל סעיף ג') כי $t - 1$ היא מילה חוקית (החסרנו את השארית העודפת וקיבלנו מילה שמתחלקת ב g ללא שארית).

ג. הוכיחו כי $d_{\min} \leq 3$.

בסעיף ב' ראינו כי $f, t - 1$ מילים חוקיות, כלומר 1100101 ו 1000110 חוקיות, אך המרחק ביניהן הוא 3.

כלומר מצאנו שתי מילים חוקיות במרחק 3, ומכאן המרחק המינימלי בין שתי מילים חוקיות קטן או שווה 3.

שימו לב: למעשה $g, 0$ הן תמיד מילים חוקיות, ולכן d_{\min} קטן או שווה מהמרחק ביניהן, כלומר מספר המקדמים שאינם אפס ב g .

לכן כאן יכולנו ישירות לקבל כי $d_{\min} \leq 3$ כיוון שב $g(x) = x^5 + x + 1$ יש 3 מקדמים שאינם אפס.

נוסחאות עזר:

שימו לב – ייתכן וחלק מהנוסחאות מיותרות.

$$617373409 \bmod 34453 = 10102$$

$$102050404 \bmod 34453 = 618$$

$$381924 \bmod 34453 = 2941$$

$$8649481 \bmod 34453 = 1778$$

$$9489665628 \bmod 34453 = 214$$

$$214913654407 \bmod 34453 = 9220$$

$$2535646388188 \bmod 34453 = 23861$$