

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

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

1. תהינה G, H חבורות סופיות כך ש $|G| = |H|$.

א. יהיו $a, b \in G$ איברים מסדר n . הוכיחו/הפריכו: גם ab הוא איבר מסדר n .

ב. יהי $\varphi: G \rightarrow H$ הומומורפיזם, הוכיחו כי φ איזומורפיזם אם ורק אם $\ker(\varphi) = \{e_G\}$.

2. תהא G תת חבורה של S_n , ותהא $H \subseteq G$ קבוצת כל התמורות בעלות סימן חיובי (זוגיות) ב G .

א. נניח שקיימת $f \in G$ תמורה בעלת סימן שלילי (אי זוגית). הוכיחו ש fH היא קבוצת כל

התמורות בעלות סימן שלילי ב G .

ב. הוכיחו שאם קיימת תמורה בעלת סימן שלילי ב G , אז כמות התמורות הזוגיות ב G שווה

לכמות התמורות האי זוגיות.

3. בוב רוצה לשלוח לאליס מסר מוצפן בשיטת RSA.

אליס פרסמה את המפתח הציבורי $n = 265$, $e = 3$.

א. חשבו את הפרמטרים הסודיים $m = \phi(n)$, $d = e^{-1} \pmod{m}$. מדוע יכולתם לעשות זאת?

ב. בוב שלח לאליס את המידע המוצפן $155 = x^3 \pmod{n}$.

מהו המידע x שבוב שלח לאליס?

4. נביט במטריצה $A = \begin{pmatrix} 0 & 1 & 1 \\ a & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}$ נתון כי הקוד הלינארי המתאים ל A מקיים כי המרחק המינימלי בין

שתי מילים חוקיות הוא $d_{\min} = 2$.

א. מצאו את a .

ב. נתון כי v הינה מילה חוקית, והמילה v' מתקבלת משגיאה אחת ב v .

נתון כי $v' = (1,1,1,1,1)$ מצאו את v .