

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.

א. יהי איבר $a \in G$ מסדר אי זוגי. הוכיחו כי קיים $b \in G$ עבורו $a = b^2$.

ב. תנו דוגמא לחבורה ואיבר $a \in G$ כך שלא קיים $b \in G$ עבורו $a = b^2$.

2. קבעו והוכיחו האם תתי הקבוצות הבאות הינן תתי חבורות של S_5 :

א. $A = \{(1), (1\ 2), (1\ 2\ 3), (2\ 3), (1\ 3\ 2)\}$

ב. $B = \left\{ (1), (1\ 2\ 3\ 4\ 5), (1\ 3\ 5\ 2\ 4), \right. \\ \left. (1\ 4\ 2\ 5\ 3), (1\ 5\ 4\ 3\ 2) \right\}$

3. בוב מעוניין שאליס תחתום לו באמצעות שיטת RSA.

המפתח הציבורי של אליס הוא $n = 2587$ ו $e = 13$.

א. אליס בחרה בטעות את אחד המספרים הראשוניים להיות מאד קטן.

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

ב. אליס חתמה עבור בוב על המידע $x = 111$ ושלחה לו את החתימה $x^d \pmod{n} = 1398$.

כיצד בוב בודק את תקינות החתימה? בצעו את החישוב (אין צורך לפתור את סעיף א' קודם).

4. נביט בפולינום $g(x) = x^3 + x^2 + 1$ המגדיר קוד פולינומי, ובמטריצה הבינארית A בגודל 3×3

המגדירה קוד לינארי.

א. קודדו את וקטורי המידע $(1, 0, 0), (0, 1, 0), (0, 0, 1)$ באמצעות הקוד הפולינומי.

ב. מצאו את המטריצה A אם נתון שהקוד הלינארי שלה זהה לקוד הפולינומי על כל וקטורי המידע

באורך 3.

נוסחאות עזר:

שימו לב – ייתכן וחלק מהנוסחאות מיותרות.

$$1954404 \bmod 2587 = 1219$$

$$1485961 \bmod 2587 = 1023$$

$$1046529 \bmod 2587 = 1381$$

$$1907161 \bmod 2587 = 542$$

$$293764 \bmod 2587 = 1433$$

$$1412763 \bmod 2587 = 261$$

$$364878 \bmod 2587 = 111$$