

קריפטוגרפיה – RSA

הנחיות הגשה:

- יש להגיש בזוגות
- תאריך הגשה : 27.5

יש לכתוב קוד בפיתון למימוש אלגוריתם RSA.
נתונים:

שני מספרים ראשוניים:

$$p=47, q=53$$

מפתח ציבורי:

$$e=5$$

כל תו בהודעה הוצפן בנפרד באמצעות המפתח הציבורי ולכן כל מספר במערך המוצפן מייצג תו אחד.

```
ciphertext = [999, 2197, 1242, 1242, 1320, 662, 2181, 1320, 785, 1242, 1634]
```

מצאו את המפתח הפרטי ופענחו את ההודעה המקורית בעזרת אלגוריתם RSA.