בס"ד

תרגיל מספר 1

(להגשה עד ל 2.6, הארכה של שבוע עד ל: 9.6)

בתרגיל זה עליכם לממש שני עצי Merkle על פי ההנחיות הבאות.

נתון ש:

- העץ הוא בינארי
- העלים הם hash של מידע שיינתן לכם.
- פונקי' ה hash בשימוש היא SHA256.

על המימוש שלכם לתמוך ב:

- הוספת עלה לעץ (קלט 1)
  - קלט: מחרוזת (עד תו ירידת שורה)
  - אין פלט
- חישוב שורש העץ הנוכחי (קלט 2)
  - קלט: אין קלט נוסף
  - פלט: שורש העץ בקידוד הקסדצימלי
- יצירת Proof of Inclusion לעלה (קלט 3)
  - קלט: מספר עלה X (העלה השמאלי ביותר מספרו 0)
  - פלט: הוכחה מעלה X לשורש העץ הנוכחי. ההוכחה היא בפורמט הבא:

  A B

  כאשר:

  A הוא שורש העץ הנוכחי

  B הוא ההוכחה. כלומר, רשימה של hashים, מופרדת על ידי תו רווח בודד, ללא שורש העץ.
- בדיקת Proof of Inclusion (קלט 4)
  - קלט: מחרוזת (המידע שמיוצג על ידי העלה) והפלט של קלט 3
  - פלט: True אם ההוכחה נכונה, אחרת False.
- יצירת מפתח פומבי ופרטי באלגוריתם RSA (קלט 5)
  - קלט: אין קלט נוסף
  - פלט: מפתח פרטי ולאחריו מפתח פומבי.

- יצירת חתימה על שורש העץ הנוכחי (קלט 6)
  - קלט: מפתח חתימה.
  - פלט: חתימה על שורש העץ הנוכחי בעזרת מפתח החתימה.
- וידוא חתימה (קלט 7)
  - קלט: מפתח וידוא, חתימה, טקסט לוידוא.
  - פלט: True אם החתימה נכונה, אחרת False.

<u>הגדרה: sparse Merkle tree.</u>

עלי העץ הם הערכים 0 או 1 (0 ברירת מחדל)

ערכי שאר הצמתים הם hash כמו בעץ מרקל רגיל.

כמות העלים (**<u>התיאורטית</u>**) היא 2^{256}.

<u>בתוספת לעיל, על המימוש שלכם לתמוך גם בsparse Merkle tree - בנפרד מעץ המרקל הרגיל:</u>

- סימון עלה - הפיכתו לבעל הערך 1 (קלט 8)
  - קלט: digest
  - אין פלט
- חישוב שורש העץ הנוכחי (קלט 9)
  - קלט: אין קלט נוסף
  - פלט: שורש העץ בקידוד הקסדצימלי
- יצירת Proof of Inclusion לעלה (קלט 10)
  - קלט: digest
  - פלט: הוכחה מהעלה הרלוונטי לשורש העץ הנוכחי. ההוכחה היא בפורמט הבא:

A B

כאשר:

A הוא שורש העץ הנוכחי

B הוא ההוכחה. כלומר, רשימה של hashים, מופרדת על ידי תו רווח בודד, ללא שורש העץ.

- בדיקת Proof of Inclusion (קלט 11)
  - קלט: digest, סיווג 0/1, והפלט של קלט 10
  - פלט: True אם ההוכחה נכונה, אחרת False.

הבדיקה יכולה להזין את כל הקלטים באיזה סדר שהיא רוצה וכמה פעמים שהיא רוצה.
בעת הזנה של קלט לא תקין יש להדפיס למסך שורה ריקה ולקלוט את הקלט הבא.
אין להדפיס שום פלטים והסברים למסך מעבר למה שהוגדר.
יש להיצמד לפלט המוגדר במדויק.
דוגמאת קלט/פלט תופיע ב submit.

<u>הגשה:</u>

- עבודה בפייתון גרסא 3 בלבד. אין אישור להשתמש בשום ספרייה, למעט hashlib עבור ביצוע ה hash בלבד וספריות הקריפטו שנלמדו בכיתה. אם יש צורך מהותי בספרייה כלשהי אחרת, יש לבקש אישור להשתמש בה.
- שאלות יש לשלוח במייל. במודל יתעדכן מדי פעם קובץ שאלות ותשובות. באחריותכם להתעדכן בו. כל הנכתב בו מחייב את כולם.
- הגשה לסאבמיט בלבד. (ולכן, חובה להקפיד על הקלט/פלט במדויק)
- ניתן להגיש לבד או בזוג (לבחירתכם). לא ניתן להגיש בשום הרכב אחר. במידה ומגישים בזוג, רק אחד מבני הזוג מגיש את התרגיל.
- השורה הראשונה בתרגיל חייבת להיות:

  # full name 1, id 1, fullname 2, id 2

  כלומר, עם שם או שמות המגישים ותעודות הזהות שלהם. חובה להקפיד על הפורמט הזה בלבד. <u>תרגיל שיוגש בלי שורה זאת בפורמט הנ"ל ירדו לו 10 נקי' מהתרגיל.</u>
- עבודה עצמית בלבד. **<u>"השראה"/שימוש בכל קוד שהוא של אחרים (כולל מהאינטרנט) אסור.</u>** דבר זה נבדק אוטו' על ידי המערכת.

בפרט אין להשתמש בשום קוד או ספרייה למימוש עץ המרקל (גם לא למימוש עץ רגיל). על כל הקוד להיות מקורי שלכם.

- יש לכלול תיעוד בסיסי. (כלומר, כל כמה שורות)

בהצלחה