בס"ד

תרגיל מספר 1

(להגשה עד ל 7.5.2020)

בתרגיל זה עליכם לממש עץ Merkle ופונקציונאליות נוספת.

נתון ש:

- העץ הוא בינארי
- מספר העלים הוא 2^i עבור $i >= 1$
- העלים הם מחרוזות
- פונקי' ה hash בשימוש היא SHA256

על העץ שלכם לתמוך ב:

- יצירת עץ מרקל מתוך רשימה של מחרוזות (קלט 1)
- יצירת Proof of Inclusion לעלה (קלט 2)
- בדיקת Proof of Inclusion (קלט 3)

כמו כן, על התוכנית לתמוך בקלט רביעי אשר מגדיר רמת קושי (מספר שלם). עליכם למצוא nonce אשר ביחד עם שורש העץ ייתן hash אשר עומד ברמת הקושי הנתונה.
קלט 5 סוגר את התוכנית.

הבדיקה יכולה להזין את כל הקלטים באיזה סדר שהיא רוצה וכמה פעמים שהיא רוצה. (למעט קלט 5 שיכול להיות מוזן רק פעם אחת בריצה).
במידה ומוזן קלט מסוג 1 יותר מפעם אחת - הוא דורס את העץ הקודם לחלוטין (העץ הקודם נמחק כלא היה ואין להתייחס אליו כלל בהמשך הקלטים).
עם זאת, שימו לב שבדיקת Proof of Inclusion לא נעשית בעזרת העץ. ולכן, גם אם הוזן כרגע למערכת רשימת מחרוזות מסוימת ויש עץ מסויים עבורה, קלט 3 יכולה להכניס איזה Proof of Inclusion שהוא רוצה - גם של עצים/מחרוזות שמעולם לא הוזנו לתוכנית.
בעת הזנה של קלט לפי סדר לא נכון יש לסגור את התוכנית.
אין להדפיס שום פלטים והסברים למסך.

דוגמאות קלט פלט:

```
1 a b c d
12a40550c10c6339bf6f271445270e49b844d6c9e8abc36b9b642be532befe94
2 1
l a r 21e721c35a5823fdb452fa2f9f0a612c74fb952e06927489c6b27a43b817bed4
3 b 12a40550c10c6339bf6f271445270e49b844d6c9e8abc36b9b642be532befe94 l a r 21e721c35a5823fdb452fa2f9f0a612c74fb952e06927489c6b27a43b817bed4
True
4 2
296 00038effdfc87247806ade69b932b51697490a9f9479ed43aef31657169e8703
5
```

שורה 1 - קלט 1 עם 4 מחרוזות מופרדות ברווח ומסתיים בירידת שורה
שורה 2 - שורש עץ הMerkle המתקבל
שורה 3 - קלט 2 עם האינדקס עבור המחרוזת השנייה (b)
שורה 4 - Proof of Inclusion כאשר l/r מסמל כיצד לבדוק את התקינות בהתאם
שורה 5 - קלט 3 עם המחרוזת שאנחנו רוצים לבדוק עבורה (b), שורש עץ ה Merkle המדובר ואז ה Proof of Inclusion
שורה 6 - ה Proof of Inclusion נכון (אם לא אזי יש לרשום False)
שורה 7 - קלט 4 עם רמת קושי של 2 אפסים מובילים
שורה 8 - ה nonce וה hash שמקיים את הדרישה
שורה 9 - סיום

<u>הגשה:</u>

- עבודה בפייטון גרסא 3 בלבד. אין אישור להשתמש בשום ספרייה, למעט hashlib עבור ביצוע ה hash בלבד. אם יש צורך מהותי בספרייה כלשהי אחרת, יש לבקש אישור להשתמש בה בפורום במודל.
- 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 נק' מהתרגיל.</u>
- עבודה עצמית בלבד. "השראה"/שימוש בכל קוד שהוא של אחרים (כולל מהאינטרנט) אסור.
- יש לכלול תיעוד בסיסי. (כלומר, כל כמה שורות)

בהצלחה