מימוש מפתח הצפנה RSA

10 בדצמבר 2022

מטרת הפרויקט:

לממש בקוד את העקרונות המתמטיים של מפתח הצפנה RSA (ראו וידאו ודף הסבר שפורסמו במודל) ולפתור בעזרת המימוש לפחות 3 מתוך 4 חידות (הגשת המימוש ופיתרון החידות במודל).
שימו לב שחלק מהחידות ניתנות לפיתרון גם לפני שמימשתם את כל הפונקציות, אז אתם יכולים לממש/לפתור באיזה סדר שאתם רוצים.

תהליך העבודה:

ביום הפרויקט יפורסמו במודל 3 קבצים:

- number_theory_functions.py כאן נמצאות הגדרות הפונקציות המיועדות למימוש: אלגוריתם אוקלידס מוכלל, העלאה בחזקה מודולו וכו'
- rsa_functions.py כאן נמצאת הגדרת ה class של מערכת rsa המשתמשת בפונקציות מהקובץ הקודם
- test_rsa.py כאן נמצאים טסטים אותם אתם יכולים להריץ כדי לוודא שהקוד שלכם עובד כמו שצריך

למה כדאי לשים לב?

- בקובץ number_theory_functions.py יש 3 פונקציות האחראיות ליצירת ראשוניים (תוך כדי שימוש באלגוריתם מילר רבין) שכבר ממומשות. אתם יכולים להשתמש בהן או בכל פונקצית ספריה אחרת לשם יצירת הראשוניים.
- בבואכם לממש את פונקצית modular_exponent (העלאה בחזקה מודולו) שימו לב שעבור מספרים גדולים העלאה ישירה בחזקה ואז לקיחת מודולו לא תסתיים בזמן אנושי סביר. לכן כדאי להשתמש בטריק הבא: אם ברצוננו לחשב $a^d \pmod n$ נוכל להביט על הייצוג הבינארי $d = \sum_{i=0}^{m} b_i 2^i$ ואז לחשב

$$a^d = a^{b_0 2^0 + \ldots + b_m 2^m} = a^{b_0 2^0} \cdot \ldots \cdot a^{b_m 2^m} \equiv_n a^{b_0 2^0} \pmod n \cdot \ldots \cdot a^{b_m 2^m} \pmod n$$

לדוגמה עבור $d = 45$ הייצוג הבינארי הוא 101101 כלומר $b_0 = b_2 = b_3 = b_5 = 1$, $b_1 = b_4 = 0$ ואז במקום לחשב a^{45} ישירות נחשב

$$a^1 \pmod n \cdot a^4 \pmod n \cdot a^8 \pmod n \cdot a^{32} \pmod n = a^{45}$$

כאשר כמובן כדאי בנוסף לבצע את המודולו n לאחר כל פעולה, דהיינו $a^{32} \equiv_n (a \pmod n)^{32}$.

הערות נוספות:

- מסתבכים עם פייתון ורוצים לממש בשפה אחרת? בסדר גמור! אומנם פייתון נוחה לחישובים עם מספרים גדולים, אך אם אתם מעדיפים להשתמש בשפת תכנות אחרת (סי/מטלב וכו) אתם מוזמנים.

- אל תשכחו לפתור את החידות ולהגיש את הפתרונות והקוד שלכם במודל. אפשר להגיש את הקבצים כזיפ או לינק לגיטהאב/דרופבוקס/דרייב וכדומה שבו הקבצים נמצאים.
- אם נשאר לכם זמן וכוח מוזמנים ליצור ממשק למערכת rsa שמיממשתם ונשמח להציג את התוצר המוגמר במודל (זוהי רשות למי שרוצה. לא חלק מדרישות הפרוייקט)

חידות (לקבלת achievement unlocked ומגן יש להגיש במודל לפחות 3 מתוך 4 החידות ואת הקוד שלכם)

החידות יפורסמו ביום הפרויקט.