1. בחר קובץ כלשהו מהמחשב- חשב עבורו את SHA1, SHA256, SHA512 ואת MD5 (נקליד את החישוב הרצוי בterminal בתוספת המילה "sum" ואת שם הקובץ הרצוי. לדוגמא "md5sum example.docx"

(או ב <https://md5calc.com/hash/md5>)

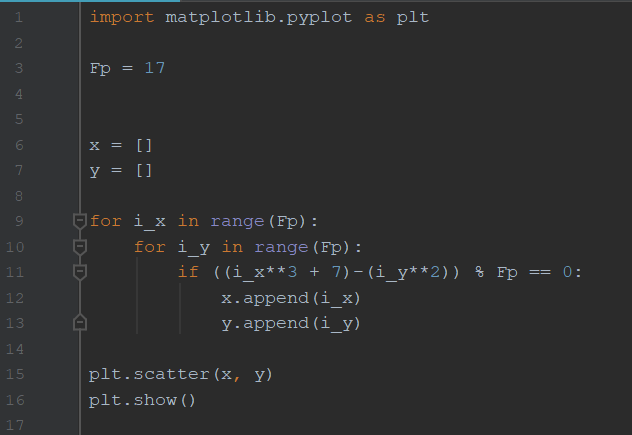
1. מדוע המפתח הפרטי והציבורי מוצפנים דווקא באמצעות SHA256? מה ההבדל בין כל סוגי הפונקציות?

גודל הפלט. מדוע משתמשים בripemd160 אח"כ?

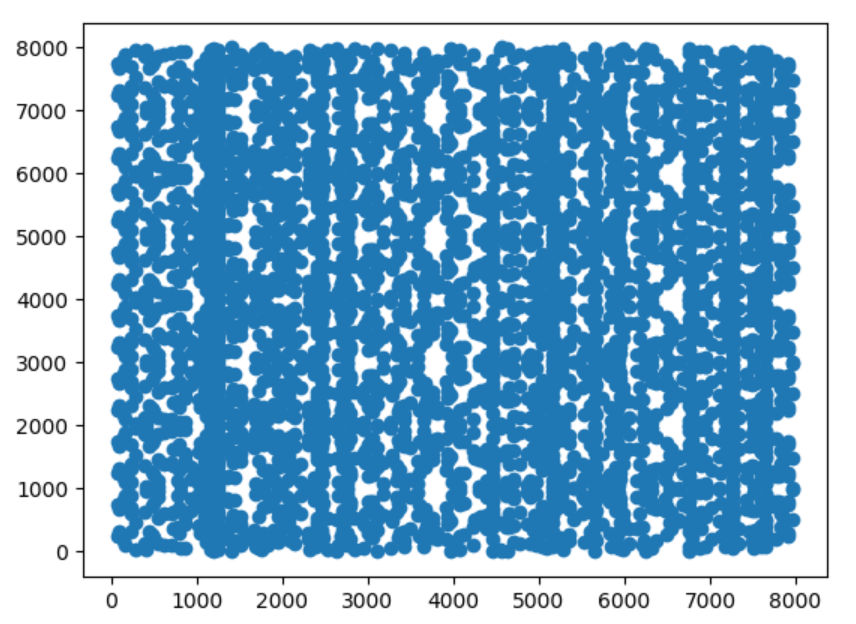
1. באפליקציות ארנק ביטקוין (ובפרט בbitcoin core) מאוחסנים זוגות של מפתחות – ציבורי ופרטי. אמרנו שאפשר לגלות את המפתח הציבורי מהפרטי. אז מדוע שלא נאכסן **רק** את המפתחות הפרטיים בארנק?

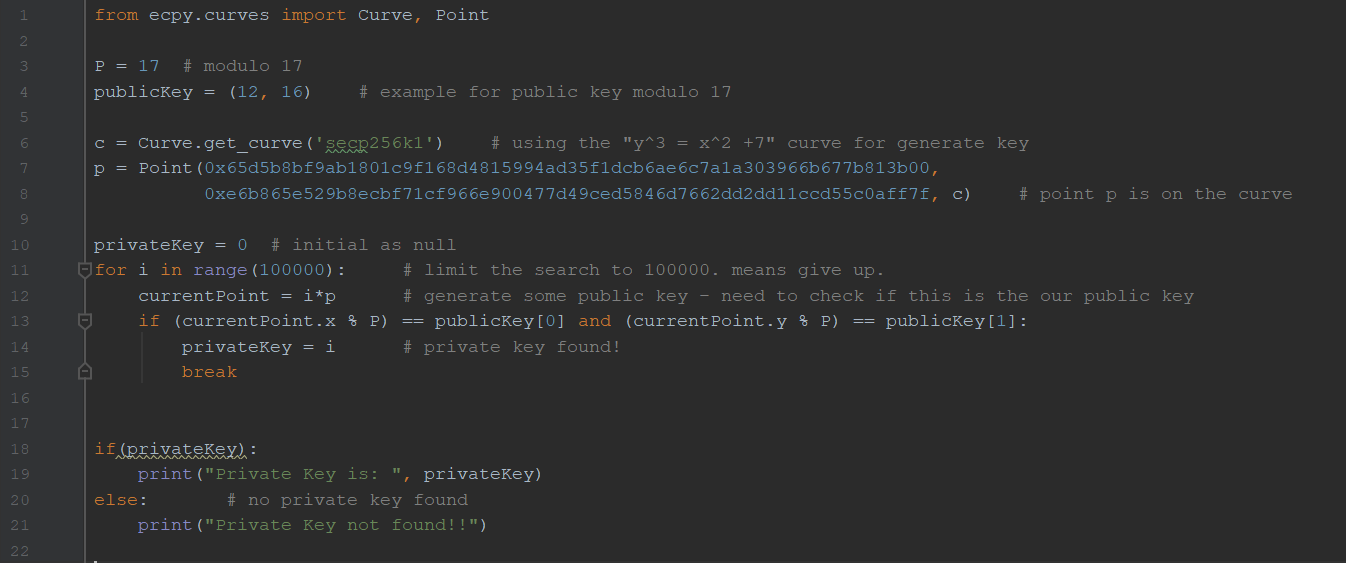
על מנת לגשת למפתח פרטי כלשהו, נצטרך את המפתח הציבורי שלנו (הוא ידוע). כיוון שהדרך ההפוכה היא אינה אפשרית בזמן סביר, נצטרך לאחסן דווקא זוגות.

1. א. כתוב תוכנה שמציירת את העקומה האליפטית secp256k1 מודולו מספר קטן (p=17 למשל).
2. עבור p=17 מצא את המפתח הפרטי עבור מפתח ציבורי (12,16) – 475
3. מאיזה מספר מודולו הפעולה נעשית מורכבת מדי?



עבור Fp=8000:





עבור p=100 המפתח הפרטי לנקודה (12, 16) הוא: 12647 (וזה לוקח בערך 10 שניות)