**Wallets**:

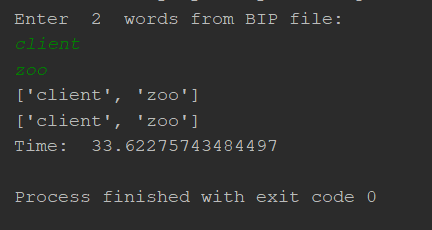
1. א. משה משתמש בארנק דטרמינסטי. הוא איבד את הארנק וכעת מנסה לשחזר את המפתחות הפרטיים שהיו לו. מה מבטיח שמשה לא ישחזר מפתחות אחרים שלא שייכים לו? הרי נוצר איזשהו שורש כללי למפתחות פרטיים.

ב. רשימת המילים שמהן יוצרים את השורש באמצעות BIP39 היא רשימה סופית (עם 2048 מילים) ואפשר לראות אותה כאן:

<https://github.com/bitcoin/bips/blob/master/bip-0039/english.txt>

מדוע אפשר להשתמש בה כדי לשחזר ארנקים ועוד צריך לשמור אותה בסוד כל כך.. האם לא יהיה קל מאוד לנסות רשימת מילים?

1. תרגיל – לפצח קוד של 2 מילים – כמה זמן ייקח לפצח קוד של 12 מילים?



1. לכתוב אלגוריתם – בהנתן seed משחזר את כל הארנק.
2. למחוק אפליקציית ארנק ולשחזר אותה באמצעות הseed.
3. האם בהנתן סיסמא ביצירת ארנק האפליקציה מבקשת סיסמא בשחזור כדי ליצור את הseed?
4. באיזה מקרים HD Wallet יהיה יעיל יותר ובאיזה מקרים לא? מה היתרון של מבנה ארנק כזה על פני האחרים? איך נעשית פעולת השחזור באמצעות עץ?

להכניס קישור לשאלה בStackexchange שההסבר מתאים לארנק סידרתי אבל איך השחזור עובד בארנק מבוסס היררכיה (עץ?) קיים קובץ cach בו שמורים המפתחות הציבוריים ששומשו.