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.
מספר האפשרויות למפתחות הוא עצום והבדלה בין אפליקציות ארנק שונות ושיטות שחזור שונות מבטיחות ייחודיות לשחזור הארנק

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? 12^{2048} אפשרויות

2. תרגיל – כתוב תוכנה הבודקת כמה זמן ייקח פיצוח של 2 מילים מתוך אוצר המילים. עבור זמן זה, כמה זמן ייקח לפצח קוד של 12 מילים?
לפצח 2 מילים לוקח בערך 33 שניות בממוצע. $(f(2) = 2^{2048} = 33sec)$
עבור זמן זה, פיצוח של 12 מילים הוא:
$$12^{2048} = (2^{3.58})^{2048} = (2^{2048})^{3.58} = (33\,\text{sec})^{3.58} = 273{,}073.719\,\text{sec} = 4{,}551.22\,\text{min} = 75.85hours = 3.16\ days$$

$$12^{2048} = (2^{2048})^6 = 33^6 sec$$
$$= 1{,}291{,}467{,}969\,\text{sec} = 21{,}524{,}466\,\text{min} = 358{,}741hours$$
$$= 14{,}947days = 498.25month = 41.52years$$

```
Enter  2  words from BIP file:
client
zoo
['client', 'zoo']
['client', 'zoo']
Time:  33.62275743484497

Process finished with exit code 0
```

3.
א. מחק ארנק בעל 3 העברות testnet לפחות, שחזר את מידע הארנק באמצעות הseed (12 המילים) – איך השחזור לוקח כל כך מהר אם נדרש לעבור על כל ההעברות?
יש מספר דרכים להאיץ את שחזור הארנק – אחת מהן היא שמירת קובץ cach על המחשב (עם הצפנת 12 המילים) וכך ניתן לשחזר במהירות.

ב. כתוב אלגוריתם – בהנתן seed בעל 12 מילים כלשהן - משחזר ארנק דטרמינסטי.
https://bitcoin.stackexchange.com/questions/42509/how-does-restoring-an-hd-wallet-work

ג. האם בהנתן סיסמא ביצירת ארנק האפליקציה מבקשת סיסמא בשחזור כדי ליצור את הseed? כן

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?
https://bitcoin.stackexchange.com/questions/74272/how-do-hd-wallets-keep-track-of-all-accounts