Digital Sign Project by Linor Dolev

1. פירוט אפשרויות usage:

```
$ ./Digital_Sign -h
```

2. יצירת זוג מפתחות (ציבורי ופרטי) תיעשה באמצעות g- ולאחריה שם המפתח
<u>דוגמא:</u>

```
$ ./Digital_Sign -g linor
```

בדוגמא זו, המפתח הפרטי ישמר בקובץ linor והציבורי ב linor.pub

3. הצפנת ופענוח קבצים:
f- המקבלת את הקובץ להצפנה
k- שם הקובץ בו שמור המפתח
e- הצפנה – הקובץ המוצפן יישמר עם הסיומת enc.
d- פענוח – הקובץ המפוענח יישמר עם הסיומת dec.

<u>דוגמא להצפנת קובץ ופענוחו:</u>

```
$ ./Digital_Sign -f example.txt -k linor -e
$ ./Digital_Sign -f example.txt.enc -k linor.pub -d
```

4. יצירת חתימה דיגיטלית באמצעות hash:
f- המקבלת את הקובץ לחתימה
k- שם הקובץ בו שמור המפתח הפרטי

ניתן לבחור אחת או יותר מפונקציות הhash הבאות:
m- Division Remainder Method
s- Folding Method
r- Digit Rearrangement Method

דוגמא להצגת כל החתימות:

```
$ ./Digital_Sign -k linor -f example.txt -msr
Division Remainder Method (mod): 130299358
Folding Method: 662619780
Digit Rearrangement Method: 1800652631
```

5. אימות חתימה דיגיטלית:
f המקבלת את הקובץ החתום
k- שם הקובץ בו שמור המפתח הציבורי

ניתן לבחור את **אחת** מפונקציות הhash הבאות, בה השתמשו לחתימה:
m- Division Remainder Method
s- Folding Method
r- Digit Rearrangement Method

v- מקבלת את ערך החתימה הדיגיטלית לאימות

<u>דוגמא כאשר הhash של האפשרות m היא 130299358:</u>

```
$ ./Digital_Sign -k linor.pub -f example.txt -m -v 130299358
Hash was validated successfully
$ ./Digital_Sign -k linor.pub -f example.txt -m -v 130299359
Hash is incorrect, file was corrupted or changed
```