234124 - מבוא לתכנות מערכות

תרגיל בית 5

סמסטר חורף 2023-24

תאריך פרסום: 28/03/2024
תאריך הגשה: 08/04/2024
מתרגל אחראי: דניאל נור

1 הערות כלליות

- הציון על תרגיל זה מהווה 4% מהציון הסופי.
- התרגיל להגשה בזוגות בלבד. חריגה מהנחיה זו רק באישור המתרגל האחראי של הקורס.
- מענה לשאלות בנוגע לתרגיל יינתן אך ורק בפורום התרגיל בפיאצה או בסדנאות. לפני פרסום שאלה בפורום אנא בדקו אם כבר נענתה – מומלץ להיעזר בכלי החיפוש שהוצגו במצגת האדמיניסטרציה בתרגול הראשון.
- שימו לב: לא תינתנה דחיות במועד הגשת התרגיל פרט למקרים חריגים. תכננו את הזמן בהתאם.
- קראו את התרגיל עד סופו לפני שאתם מתחילים לממש. חובה להתעדכן בפורום הפיאצה, הכתוב שם מחייב.
- העתקות קוד בין סטודנטים ובפרט גם העתקות מסמסטרים קודמים תטופלנה. עם זאת – מומלץ ומבורך להתייעץ עם חברים על ארכיטקטורת המימוש
- המסמך נכתב בלשון זכר מטעמי נוחות בלבד ומיועד לשני המינים.
- מטרת תרגיל זה היא היכרות עם תכנות ב-Python.

2 מערכת הצפנה ופענוח

2.1 רקע

גנדלף האפור, בוגר קורס מת"ם, רוצה לזמן ישיבה דחופה בריוונדל כדי לדון כיצד יש לנצח את כוחות האופל אשר רוצים שהוא יכשל בקורס. על מנת למנוע מכוחות האופל לקרוא את ההודעה לגבי מועד ומיקום הפגישה ולתקוף את ריוונדל, גנדלף החליט להצפין את ההודעה.
לצערו, גנדלף עסוק כרגע במסע להר הבודד ואינו יכול לכתוב את התוכנה שתצפין ותפענח עבורו את ההודעה, ולכן הוא פנה אליכם בבקשה שתעזרו לו לכתוב תוכנת הצפנה משוכללת.

2.2 קצת על צפנים

צופן (Cipher) הוא זוג אלגוריתמים ("הצפנה" ו-"פענוח") אשר מקבלים כפרמטר מחרוזת ומידע נוסף (אשר נקרא "מפתח") ומחזירים מחרוזת.

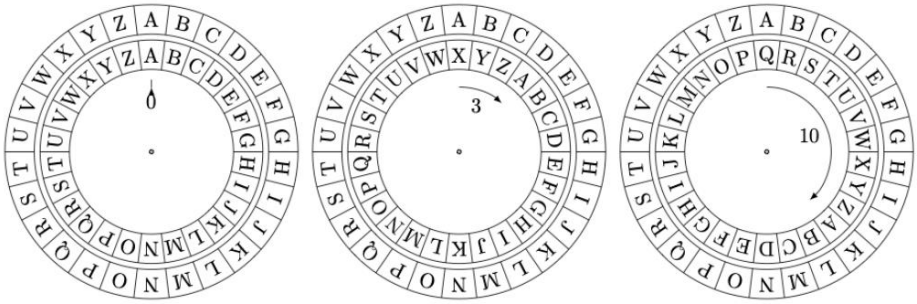
הצפנה היא אלגוריתם אשר, בעזרת שימוש במפתח, מחזיר מחרוזת חדשה אשר מקודדת בתוכה את המחרוזת המקורית באופן שקשה לשחזר ממנו את המחרוזת המקורית ללא ידיעת המפתח.

פענוח הוא אלגוריתם אשר, בעזרת שימוש באותו מפתח כשל ההצפנה, מחזיר את המחרוזת המקורית בהינתן המחרוזת המוצפנת.

כלומר- מתקיים כי הצפנה של מחרוזת ופענוח של המחרוזת המוצפנת לפי אותו מפתח מחזירים את המחרוזת המקורית: $\text{decrypt}(\text{encrypt}(M,K),K) = M$.

בתרגיל זה נתמקד בצפנים אשר מצפינים כל תו במחרוזת בנפרד והמחרוזת המוצפנת היא שרשור הצפנות התווים.

אם הנושא של צפנים לא ברור לכם לחלוטין בשלב זה, לא נורא. זאת לא מטרת התרגיל. תוכלו לקחת בהמשך את הקורסים 236350 הגנה ברשתות ו-236506 קריפטולוגיה מודרנית.



2.3 צופן קיסר

גנדלף למד קצת היסטוריה, ובמיוחד מעניין אותו יוליוס קיסר מהאימפריה הרומית. לפי הסיפורים, יוליוס קיסר השתמש בצופן הנקרא צופן קיסר[1] (או הסטה קיסרית, צופן היסט...) ובאנגלית Caesar Cipher.

[1] על שמו של יוליוס קיסר כמובן

ראשית, נתאר כיצד פועל צופן קיסר באופן לא פורמלי:

ה**מצפין** מקבל מחרוזת כלשהי s וערך הזזה $k \in \mathbb{Z}$ (המפתח). עבור כל תו $c \in s$, המצפין יבצע k הזזות של c בכיוון המתאים (לפי הסימן של k – אם k חיובי יוזז ימינה ושלילי שמאלה). למשל, אם $k = 2$, וקיבלנו את התו 'A', אז נזיז אותו פעמיים – פעם אחת ל-'B', ופעם שנייה ל-'C'. הערך 'C' אפוא הוא הערך המתקבל מהצפנת 'A' עם מפתח 2 לפי צופן קיסר.

<u>הערות:</u>

1. הזזות מתבצעות כך שהתווים מסודרים במעין מעגל. כלומר, אחרי Z יש A, לאחר מכן B וכן הלאה.
2. אנו מתייחסים לאותיות גדולות וקטנות **בנפרד**, כלומר לאחר הצפנה אות קטנה תישאר אות קטנה ואות גדולה תישאר אות גדולה.
3. מצפינים רק אותיות אנגליות גדולות וקטנות, כל שאר התווים נשארים ללא שינוי (לכל תו c שאינו A עד Z או a עד z, תוצאת ההצפנה של c היא c בלי תלות במפתח).

דוגמאות נוספות:

$$\text{encrypt}(\text{a}, 2) = c, \qquad \text{encrypt}(\text{A}, 2) = \text{C},$$
$$\text{encrypt}(\text{K}, -2) = \text{I}, \qquad \text{encrypt}(\text{A}, -2) = \text{Y}$$

נזכור שהגדרנו שתוצאת הצפנה (או פיענוח) של מחרוזת היא שרשור תוצאות ההצפנה (או הפענוח) של התווים במחרוזת. למשל, $\text{encrypt}(\text{aB}, 2) = \text{cD}$.

ה**מפענח** מקבל מחרוזת מוצפנת כלשהי s' וערך הזחה $\text{k} \in \mathbb{Z}$. עבור כל תו $c' \in s'$, המפענח יבצע k הזחות של c' בכיוון המנוגד לכיוון ההצפנה.

למשל:

$$\text{decrypt}(\text{c}, 2) = \text{a}, \qquad \text{decrypt}(\text{C}, 2) = \text{A},$$
$$\text{decrypt}(\text{I}, -2) = \text{K}, \qquad \text{decrypt}(\text{Y}, -2) = \text{A}$$

הבחנה חשובה: $\text{decrypt}(M, k) = \text{encrypt}(M, -k)$. כיצד ניתן להשתמש בעובדה זו כדי להימנע משכפול קוד?

מימוש צופן קיסר

ממשו את המחלקה `CaesarCipher` אשר מכילה את המתודות הבאות:

1. בנאי המקבל מספר כמפתח.
2. <u>`encrypt`</u>: אשר מקבלת מחרוזת ומחזירה את ההסטה הקיסרית של המחרוזת לפי המפתח של העצם עליו מופעלת המתודה.
   דוגמאות:

```
>>> caesar_cipher = CaesarCipher(3)
>>> caesar_cipher.encrypt('a')
'd'
>>> caesar_cipher.encrypt('Mtm is the BEST!')
'Pwp lv wkh EHVW!'
```

3. <u>`decrypt`</u>: אשר מקבלת מחרוזת ומחזירה את הפענוח של המחרוזת שהוצפנה באמצעות צופן קיסר לפי המפתח של העצם עליו מופעלת המתודה.

דוגמאות:

```
>>> caesar_cipher.decrypt('d')
'a'
>>> caesar_cipher.decrypt('Pwp lv wkh EHVW!')
'Mtm is the BEST!'
```

4. `key_shift`: אשר מקבלת מספר `delta` ומקדמת את המפתח של העצם לפי `delta`. למשל, אם מפתח העצם היה 3 וקראנו למתודה עם הפרמטר 2, מאותה נקודה העצם יצפין/יפענח עם המפתח 5.

דוגמאות:

```
>>> caesar_cipher2 = CaesarCipher(2)
>>> caesar_cipher2.key_shift(3)
>>> caesar_cipher2.encrypt('a')
'f'
```

2.4 צופן ויז'נר (Vigenère)

גנדלף הלבן למד על צופן קיסר, אבל הוא חושב שהצופן חלש מידי וכוחות האופל יצליחו לפענח אותו בקלות.
לכן, גנדלף המשיך הלאה בלימודי ההיסטוריה שלו עד שלמד על צופן ויז'נר (שפותח באיטליה במאה ה-16).

בצופן החדש, המפתח יכיל **רשימה של ערכים** (ולא ערך בודד) כאשר כל אות בטקסט המוצפן תוצפן באמצעות מפתח מתוך רשימת המפתחות בצורה מחזורית.

למשל, עבור המחרוזת "come to Rivendell!" והמפתח [7,8,11,13, −2,4] נקבל כי המחרוזת המוצפנת תהיה:

c	o	m	e		t	o		R	i	v	e	n	d	e	l	l	!
+7	+8	+11	+13		-2	+4		+7	+8	+11	+13	-2	+4	+7	+8	+11	
j	w	x	r		r	s		Y	q	g	r	l	h	l	t	w	!

כלומר - "jwxr rs Yqgrlhltw!"

<u>הערה:</u> בדומה לצופן קיסר, בצופן ויז'נר מצפינים רק אותיות אנגליות גדולות וקטנות, כל שאר התווים נשארים ללא שינוי. בצורה דומה, הפענוח של מחרוזת גם הוא יבוצע אות–אות באמצעות מפתח מרשימת המפתחות.

למשל, עבור הדוגמא לעיל, עבור המחרוזת המוצפנת "jwxr rs Yqgrlhltw!" והמפתח [7,8,11,13, −2,4] נקבל:

j	w	x	r		r	s		Y	q	g	r	l	h	l	t	w	!
+7	+8	+11	+13		-2	+4		+7	+8	+11	+13	-2	+4	+7	+8	+11	
c	o	m	e		t	o		R	i	v	e	n	d	e	l	l	!

מימוש צופן ויז'נר

ממשו את המחלקה `VigenereCipher` אשר מכילה את המתודות הבאות:

1. בנאי המקבל רשימה של מספרים כמפתח
2. `encrypt`: אשר מקבלת מחרוזת ומחזירה את ההצפנה של המחרוזת לפי המפתח של העצם עליו מופעלת המתודה (בשיטת צופן ויז'נר).
3. `decrypt`: אשר מקבלת מחרוזת ומחזירה את הפענוח של המחרוזת שהוצפנה בהצפנת ויז'נר לפי המפתח של העצם עליו מופעלת המתודה.

דוגמאות:

```
>>> vigenere_cipher = VigenereCipher([3])
>>> print(vigenere_cipher.encrypt('l'))
o
```

```
>>> vigenere_cipher = VigenereCipher([2, -4, -14, -16, -17, -17])
>>> print(vigenere_cipher.encrypt('we wish you best of luck in all of your exams'))
ya isbq akg lnbv kr vdlm ez kuu qb kyda gtmwb
>>> print(vigenere_cipher.decrypt('ya isbq akg lnbv kr vdlm ez kuu qb kyda gtmwb'))
we wish you best of luck in all of your exams
```

```
>>> vigenere_cipher = VigenereCipher([1,2,3,4,-5])
>>> print(vigenere_cipher.encrypt('Hello World!'))
Igopj Xqupy!
>>> print(vigenere_cipher.decrypt('Igopj Xqupy!'))
Hello World!
```

2.5 מימוש המערכת

בחלק זה נממש את המערכת בה גנדלף ישתמש להצפנת ופענוח ההודעות שלו.

ממשו את הפונקציה `loadEncryptionSystem(dir_path, plaintext_suffix)` אשר מקבלת נתיב לתיקייה[2] שבה יש קובץ בשם config.json אשר בו שמורים המזהים הבאים:

- `type`: מחרוזת בעלת אחד משני הערכים הבאים: `"Caesar"/"Vigenere"`, אשר מגדירה באיזה סוג הצפנה עלינו להשתמש.
- `encrypt`: ערך בוליאני המיוצג כמחרוזת (`"True"/"False"`) אשר מגדיר אם נצפין או נפענח (נצפין כאשר הערך הוא אמת ונפענח אחרת).
- `key`: מפתח שבאמצעותו נצפין/נפענח. אם שיטת ההצפנה היא Caesar הוא יהיה מספר, אם השיטה היא Vigenere הוא יהיה רשימה של מספרים.

הפונקציה תטען את הקובץ ותיצור מערכת מתאימה, ואז תבצע את הפעולה המתוארת ב-config על כל הקבצים בתיקייה (באופן לא רקורסיבי) באופן המתואר כאן. הפונקציה לא תמחק את הקבצים המקוריים אלא רק תיצור קבצים חדשים.

---

[2] directory, folder, ספריה

אם הפעולה הדרושה היא הצפנה, הפונקציה תצפין כל קובץ בתיקייה עם סיומת plaintext_suffix (כלומר בעל שם מצורה `filename.<plaintext_suffix>`) לקובץ בעל שם זהה אך עם סיומת enc.

אם הפעולה הדרושה היא פענוח, הפונקציה תפענח כל קובץ בתיקייה בעל סיומת '.enc' לקובץ בעל שם זהה אך עם סיומת `plaintext_suffix`.

הערה: במידה ואנו מצפינים/מפענחים בשיטת צופן ויז'נר בהצפנה של כל קובץ עלינו להתחיל מתחילת המפתח.

<u>רשות (לא ייבדק):</u> נסו לממש את המחלקות Caesar ו-Vigenere באמצעות ירושה בפייתון כפי שראינו בתרגול.

<u>דגשים נוספים:</u>

- בסעיף זה אתם רשאים להשתמש בספריה os ובכל ספריה אחרת שנלמדה בקורס.
- ירידת שורה נחשבת כמו כל תו שאינו אות מבחינתנו – נשארת כפי שהיא לאחר הצפנה/פענוח

3 הערות

- בכל התרגיל אין להשתמש במספרי קסם למעט 0/1
- ניתן להניח כי הקלט תקין בכל התרגיל (שימו לב שהמחרוזות להצפנה/פענוח יכולות להכיל כל תו ולא רק אותיות)
- וודאו כי אתם מריצים פייתון גרסה 3.6. שימו לב כי גרסה זו אינה גרסה ברירת מחדל על השרת. כדי להריץ פייתון 3.6 <u>השתמשו בפקודה python3</u>
- פתרון התרגיל צריך לעבוד בכל מערכת הפעלה (platform independent).
- מסופקים לכם עם התרגיל מספר טסטים אשר נועדו לבדוק בכלליות את התוכנית שלכם.
  - אל תסתמכו על טסטים אלו! כתבו טסטים ובדקו את התוכנית שלכם
- כרגיל, ישנו קובץ finalcheck בנתיב ~mtm/public/2324a/ex5 על השרת

4 הגשה

את ההגשה יש לבצע דרך אתר הקורס, תחת:

Assignments → HW5 → Electronic Submit

הקפידו על הדברים הבאים:

- יש להגיש את קבצי הקוד מכווצים לקובץ zip (לא פורמט אחר).
- אין להגיש קבצים נוספים מלבד קובץ אחד בשם ex5.py בתוך הזיפ.
- ניתן להגיש את התרגיל מספר פעמים, רק ההגשה האחרונה נחשבת .
- על מנת לבטח את עצמכם נגד תקלות בהגשה האוטומטית, שימרו את קוד האישור עבור ההגשה. עדיף לשלוח גם לשותף. כמו כן שימרו עותק של התרגיל על חשבון ה– Google Drive/GitHub/CSL3 שלכם לפני ההגשה האלקטרונית ואל תשנו אותו לאחריה (שינוי הקובץ יגרור שינוי חתימת העדכון האחרון)
  - כל אמצעי אחר לא יחשב הוכחה לקיום הקוד לפני ההגשה .

בהצלחה !

بالنجاح !

! LUCK GOOD