תרגיל מספר 1.

להגשה עד לתאריך: 23.5.
הארכה למעוניינים עד לתאריך: 30.5.
ההארכה כוללת כל בלת״ם, מחלות וכו׳.
לא ניתן יהיה להגיש לאחר תאריך זה כלל.

בתרגיל זה עליכם לכתוב סקריפט הממש את התקפת ה Padding oracle attack.

שלב 1:
נשתמש בפייתון גרסא 3 ובספריית pycryptodome
וודאו שהספרייה עובדת ורצה תקין. (התקנה בעזרת pip3).

נשתמש בimportים הבאים:

```
from Cryptodome.Cipher import DES
from Cryptodome.Util.Padding import pad,unpad
```

הimport הראשון יאפשר לנו לבצע הצפנה בעזרת צופן הבלוקים DES.
הimport השני יאפשר לנו לבצע ריפוד (ולהוריד ריפוד).

שלב 2:
עליכם לרפד את המחרוזת Hello World כך שתהיה בגודל 16 בתים.
כלומר, על המחרוזת המרופדת להיראות כך: (בהדפסה)

```
b'Hello World\x05\x05\x05\x05\x05'
```

שלב 3:
עליכם להצפין בעזרת DES במצב CBC את המחרוזת המרופדת בעזרת המפתח poaisfun ובעזרת IV שכולו אפסים. (תזכורת: גודל בלוק ב DES הינו 8 בתים).
כלומר, לאחר הצפנה, הciphertext צריך להיות מורכב מהבתים הבאים: (מוצגים ב hex)

```
0x33
0xaa
0xa3
0x1
0x7e
0x45
0x33
0x7b
0xd3
0x63
0x42
0xb3
0x92
0xb
0xe6
0x56
```

שלב 4:

עליכם לוודא שאתם יכולים לפענח את הciphertext ולבטל את הריפוד ולקבל בחזרה את הplaintext.

שלב 5:

כיתבו פונק׳ בשם xor אשר מקבל 3 פרמטרים ומחזירה את הxor שלהם.
למשל, הרצת הקוד הבא:

```
print(xor(0,0,0))
print(xor(0,0,1))
print(xor(0,1,0))
print(xor(0,1,1))
print(xor(1,0,0))
print(xor(1,0,1))
print(xor(1,1,0))
print(xor(1,1,1))
```

ידפיס:

```
b'\x00'
b'\x01'
b'\x01'
b'\x00'
b'\x01'
b'\x00'
b'\x00'
b'\x01'
```

שלב 6:

כתבו פונק׳ בשם oracle אשר מקבלת ciphertext, מפתח ו iv, ומבצעת פיענוח ומבטלת את הריפוד.
אם הפעולה הצליחה - היא מחזירה True, אחרת False.
למשל, אם תזינו את הciphertext שיצרתם היא תחזיר True, אבל אם תשנו אותו בצורה כלשהי היא תחזיר False.

שלב 7:

צרו משתנה בשם c שהוא שרשור של בלוק מאופס והבלוק השני של הciphertext.
כלומר, המשתנה c צריך להיות מורכב מהבתים הבאים: (מוצגים ב hex)

```
0x0
0x0
0x0
0x0
0x0
0x0
0x0
0x0
0xd3
0x63
0x42
```

0xb3
0x92
0xb
0xe6
0x56

<u>שלב 8:</u>
שלחו את c לאורקל בלולאה, כל פעם הגדילו את הבית השמיני ב1, עד אשר האורקל מחזיר True.

<u>שלב 9:</u>
השתמשו במשוואה מהמצגת ובפונק׳ הxor שכתבתם כדי לחלץ את הבית האחרון בבלוק השני המוצפן. (צריך להיות 0x05)

<u>שלב 10:</u>
השתמשו במשוואה מהמצגת ובפונק׳ הxor שכתבתם כדי לשנות את c כך שהבית האחרון יפוענח להיות 0x02

<u>שלב 11:</u>
הפכו את שלבים 8-10 ללולאה, אשר כל פעם חושפת בית, עד שהיא חושפת את כל הבלוק.

<u>שלב 12:</u>
הפכו את שלב 11 ללולאה אשר יודעת לחשוף את כל הciphertext, בלוק אחר בלוק.

לבסוף, התוכנית שלכם תקבל 3 ארגומנטים.
ארגומנט ראשון ciphertext, ארגומנט שני מפתח וארגומנט שלישי iv (כולם יוזנו בהקסה דצימלי, הciphertext יכול להכיל כמה מספר בלוקים לא ידוע, הארגומנטים יופרדו ברווח).

עליכם להדפיס למסך את הplaintext המקורי **<u>כולו</u>** בעזרת ההתקפה, יש להדפיס את הplaintext בצורה טקסטואלית.
<u>אסור</u> להשתמש במפתח בשביל לפענח את הciphertext, אלא רק למימוש הoracle.
אי הקפדה על הנחיה זו תגרור ציון 0 בציון התרגול בקורס.

הגשה ביחידים או בזוגות, לבחירתכם.
יש להגיש את קובץ הקוד (היחיד) למודל. יש לקרוא לקובץ ex1.py (בדיוק ככה).
יש להוסיף קובץ pdf (פורמט pdf בלבד - כל פורמט אחר לא יתקבל) המדגים הרצה של הסקריפט - כולל הסבר שלכם של כל שלבי הקוד וההרצה.
<u>הסבר ברור ומפורט המראה הבנה של שלבי ההתקפה והמימוש שלכם.</u>

יש להגיש למודל קובץ טקסט בשם details.txt עם שמות ות.ז. של המגישים. שימו לב, חובה על הקובץ להיות בפורמט הבא:

Israel Israeli 123456789
Israela Israeli 012345678

בלי רווחים נוספים, בלי שורות נוספות, ובשפה האנגלית בלבד. אי הגשה של קובץ ה details.txt הנ״ל או הגשתו באופן שונה ממה שהוגדר, **<u>תגרור הורדה של 20 נקודות בציון התרגיל.</u>**
עבודה עצמאית בלבד. הנושא ייבדק ויאכף.

בהצלחה