**רעיון לצופן שקל להמציא וקשה לפענח.**

מצד שני אם יש כיוון אפשר בעזרת תוכנית לפצח אותו.

מפתח הצופן יהיה אוסף של 8 ביטים לפי סדר ומצב שניקבע, למשל:
00111010

כדי לקודד תוים, נמצא את הייצוג ה- ASCII של התו (הפונקציה ord בפייתון למשל) - נסב את הערך

למספר בינארי (אפשר ליצג עד 256 בשמונה ביטים) ועבור כל תו נבצע את הפעולה: XOR בין התו

בבינארי והמפתח שלנו.

הפעולה XOR זה קיצור של: Exclusive Or שזה אומר אם שני הביטים שונים, התוצאה 1, אחרת אפס.
זו טבלת האמת של XOR

| XOR | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 1 | 0 |

דוגמה:

נניח שרוצים לקודד את המילה: Hello

| Letter | ASCII -dec | Binary | (After XOR with 00111010) | ASCII back | Char |
|---|---|---|---|---|---|
| H | 72 | 01001000 | 01110010 | 114 | r |
| e | 101 | 01100101 | 01011111 | 95 | _ |
| l | 108 | 01101100 | 01010110 | 86 | V |
| l | 108 | 01101100 | 01010110 | 86 | V |
| o | 111 | 01101111 | 01010101 | 85 | U |

כלומר המחרוזת Hello לאחר הקידוד תהיה:

r_VVU

להפוך ממחרוזת ביטים למספר דצימלי אפשר להשתמש בפונקציה: int כך:

int(' 01110010' , 2) ==> 114

להפוך מעשרוני לבינארי אפשר להשתמש בפונקציה: bin, לדוגמה:

bin(114) ==> '0b1110010'

bin מחזירה עם קידומת 0b ומחזירה את הגודל המדוייק (לפעמים צריך להשלים משמאל באפסים).

לחשוב על: אם לא ידוע הצופן, איך אפשר לכתוב תוכנית שתמצא אותו?