מבוא להצפנה: לתרגיל מס' 2.

בשאולות הבאות הציון ייקבע על ידי לא רק על ידי התוצאה אלא גם על ידי השיטה. אסור להשתמש בכוח גס וצריך לתאר את הדרך, כולל הנסיונות שנכשלו . אסור להשתמש באתרים שמפענחים בשבילכם את הצפנים. מוצר להשתמש בקוד שמחשב שלב (למשל, סופר תדירות האותיות). מותר לכתוב קוד בזוגות או בקבוצות של 3, אבל צריך לציין עם מי עבדתם. תעלו את הקוד ביחד עם התרגיל (אפשר ב-pdf). באופן כללי, הבודק חייב להבין בקלות איך פתרתם את התרגיל. לתדירות האותיות באנגלית, השתמשו בערכים:

englishLetterFreq = {'E': 12.70, 'T': 9.06, 'A': 8.17, 'O': 7.51, 'I': 6.97, 'N': 6.75, 'S': 6.33, 'H': 6.09, 'R': 5.99, 'D': 4.25, 'L': 4.03, 'C': 2.78, 'U': 2.76, 'M': 2.41, 'W': 2.36, 'F': 2.23, 'G': 2.02, 'Y': 1.97, 'P': 1.93, 'B': 1.29, 'V': 0.98, 'K': 0.77, 'J': 0.15, 'X': 0.15, 'Q': 0.10, 'Z': 0.07}

1. פענחו את ההודעה הבאה שהוצפנה על ידי צופן ויג'נר עם מפתח של לכל היותר 6 אותיות.

WERXEOFBTKPKGBXUTPNIVFEGTRYWGXHVPGXFRJBHUKCMVNLQXOGCWIHGEAGRRKGDGYYGR
AKJRWXRIMRXUJMUVQETTKVZLVHTUGCTTPGCYQIKPMKFLRTNCCSINRGCMGORXGVFSCBPKC
AEKXGQEGWMGFERJAXFTGEAGIRTQVUCRKAGRXHPZQIAGICKXTJCXGQKFTKYFPSLOFTXGIW
PDFVYCJGKERTENZEXUNVAXIJVPIXZKZPVMKMEECZLIXZKYRBRYCGHTTWEAGIGHTRRGGHH
RJVHTZRWFUKFPMEICPMGKFTXPTPNIVZMCTPURWXTVTTKUZLVWGTPNIVZMCMJVBTMCZJTW
QGCGTVZMCHHRAXIJVPXLEFLIKQCJTWDFRWUAKFTTNXMGBVYKPGFZLTTEYGCLVRLRXDPYZ
XAKFTDGPGHTUVAGXVZBTTNCWZGQNLDGNPRDMJVADFOLLXVCERHNULYAEARQWHTKQIKKEE
DYEYYGTEKCGLYYGRAKJLTXFVBIHFVAGRRKRWXEZNWXTKCMMHFPBTNCWPVTPNIHUPQIXOZ
QIAGFPSXTVBABUKMUXNVKTGVJMUYKEGIXRFQHBDCCEECZLIXZKQUBPZRTIQJQXUNVANIJ
VPIXZKQUBPZRTIQJQXUNVITRURLSMJVCCVTPNIBQEYCWFVAGRRKGDGCCEDKKKFBLYYGRA
EFPGXUGMCWVFCPVJBCNDGPQPKGZKEHTKYCMDFRWYQIKPENPYCWKEYRMWRJEKCTRXVGRQR
BRYCGLYZRWHWKTPKKRZAXMVWHVCEZTMTZTXTNCWQKQBCCPKKFDGNPRWXMEMLEGUETHHKF
TVKGFTKWJCSTPUYGXVYCGXHFPTNUVJTLUFPTOGEADNPKCGITFBJVVZTTYQIKDLVGSGIQJCH

2. ארבע ההודעות הבאות הוצפנו מאותה הודעה, בצופן הזזה, צופן אפיני, צופן ויג'נר וצופן היל עם מטריצות בגודל 2 (לא בהכרח בסדר הזה). פענחו את ההודעה ומצאו את מפתח ההצפנה ומפתח הפענוח של כל אחד מה צפנים.
   a. M1: GCKAMBYBUSJLYTDJUQLUQUUGUNLFHYZBLJUF
   b. M2: HRQVKWTMOHVUTYHOYTGDURYVZUVULHYMVOYQ
   c. M3: LNSTWODMCLTYDELCEDQFYNETZYTYRLEMTCES
   d. M4: GOMNFYNTIHDBPPZPONSJGBKVPFDBMEPYPDHO

3. ההודעה הבאה הוצפנה על ידי צופן אוגר הזזה לינאיר (LFSR):
   01100 01010 11100 11101 01000 10001 10001 01011 10011 10101

ידוע כי תחילת הודעת המקור הוא 10010 01001 00101.

מצאו את שאר הודעת המקור ואת נוסחת הנסיגה היוצרת המפתח. מה הוא אורך המחזור של סדרת הסיביות שהיא נוצרת? האם זה אורך המחזור המקסימלי עבור נוסחת נסיגה מאורך זה?

בהצלחה!