11. בשאלה זו ארבעה סעיפים, א–ד, שאין ביניהם קשר. יש לענות על כל הסעיפים.

א. המסר: It's my bank account הומַר לסיביות (ביטים), חוץ מן המילה my .

המירו את המילה my לסיביות.

הערך ה־ Ascii של האות m הוא 109 בבסיס עשרוני, והערך ה־ Ascii של האות y הוא 121 בבסיס עשרוני.

ב. להלן אוסף סיביות – m , המייצג את הערך ה־ Ascii של המילה Hey , ואוסף סיביות – key , שהוא פנקס חד־פעמי (OTP).

m – 010010000110010101111001

key – 110110100100010111101101

הַצפינו את המילה Hey באמצעות הפעולה xor עם key .

ג. רונית ויובל הצפינו מסר כלשהו – m , שאורכו n הוא זוגי, באמצעות הפעולה xor עם מפתח – key , וקיבלו מסר מוצפן – cipher . למען הזהירות, הם חצו את key לשניים. את החצי הראשון של המפתח, key_1 (שהוא באורך n/2), לקחה רונית איתה למקום אחד, ואת החצי האחר – key_2 (שהוא באורך n/2), לקח איתו יובל למקום אחר.

כדי לפענח את המסר, ביצעה חברתם הלית את הפעולות האלה לפי הסדר:

- היא לקחה מיובל את key_2 , והוסיפה לתחילתו כמות של אפסים באורך של n/2 (וכך נהיה אורכו של key_2 באורך n).
- היא ביצעה cipher xor key_2 וקיבלה אוסף סיביות. נקרא לאוסף שהיא קיבלה halfMessage .
- היא לקחה מרונית את key_1 , והוסיפה לסופו כמות של אפסים באורך של n/2 (וכך נהיה אורכו של key_1 באורך n).
- היא ביצעה halfMessagae xor key_1 וקיבלה אוסף סיביות. נקרא לאוסף שהיא קיבלה fullMessage .

כִּתבו אם הפענוח תקין (כלומר, אם fullMessage הוא המסר m). נמקו.

הערה: תשובה ללא נימוק לא תזוכה בנקודות.

ד. בוב ואליס השתמשו בפעולה CreatePrg/createPrg כדי לייצר מפתח PRG , ואיתו הצפינו מסר באמצעות הפעולה xor . הפעולה מקבלת מחרוזת של סיביות – seed , ואת אורך המסר שרוצים להצפין – len , ומחזירה פנקס חד־פעמי (OTP).

הפעולה CreatePrg/createPrg כתובה לפניכם בשפות Java ו־ C# .

איב יודעת מהי הסיבית האחרונה של ה־ seed . האם היא יכולה לפצח את המסר בניסיון אחד? נמקו.

הערה: תשובה ללא נימוק לא תזוכה בנקודות.

בשפת **Java** :	בשפת **C#** :

public static String createPrg (String seed, int len) {
  String str;
  if (seed.charAt(seed.length() -1) == '1')
  str="0";
  else
  str="1";
  for (int i = 1; i < len; i ++) {
  if (str.charAt(str.length() -1) == '0')
  str += "1";
  else
  str += "0";
  }
  return str;
}
	public static string CreatePrg (string seed, int len) {
	  string str;
	  if (seed[seed.Length -1] == '1')
	  str="0";
	  else
	  str="1";
	  for (int i = 1; i < len; i ++) {
	  if (str[str.Length -1] == '0')
	  str += "1";
	  else
	  str += "0";
	  }
	  return str;
	}