לפניכם/ן שתי חידות. פיתרו את החידות והעלו את התשובות לטופס שבאתר.

בין הפותרים נכונה כל שאלה יוגרל פרס: אוזניות אלחוטיות Jabra 45t

שאלה 1:

כולנו זוכרים את שירו המפורסם של של יזהר כהן, אבניבי אובובהבב, שהשתמש בשפת הסתרים בה כל אות שניה מוחלפת באות ב. https://www.youtube.com/watch?v=WiyF9tv2ocs
לדוגמא, המשפט "אני אוהב" מוחלף במשפט "אבניבי אבובהבב".

בוב דובר אנגלית בריטית, ולכן הוא מדבר בשפת ה B ומוסיף לאחר כל אות את האות B. לדוגמא, במקום לומר hello הוא אומר hbeblblbob
אליס דוברת אנגלית אמריקאית, ולכן היא מדברת בשפת ה A ומוסיפה לפני כל אות את האות A. לדוגמא, במקום לומר hello היא אומרת ahaealalao.
ביתר דיוק, הקידוד שהם מבצעים מתבצע בצורה הבאה:

- כל האותיות הן lower case
- בין כל שתי מילים יש רווח אחד בלבד, ואין סימני פיסוק.
- לא מוסיפים אות בסוף מילה, אבל הרווח שבין שתי מילים מוחלף בצמד האותיות bb אצל בוב, ובצמד האותיות aa אצל אליס.
- לדוגמא, כך יהיה קידוד המשפט hi there
- בוב: hbibbbtbhbebrbeb
- אליס: ahaiaaatahaearae

אליס ובוב מדברים בו זמנית, ודבריהם מכסים זה את זה. גדי מאזין להם ושומע את החיבור של דבריהם. החיבור מוגדר כסכום המספרים הסידוריים של האותיות בתוספת 13 מודולו 26, כלומר לכל אות מוגדר מספר סידורי: a=0,b=1,…,z=25 וכאשר מחברים אותיות מבצעים חיבור של המספרים הסידוריים, מוסיפים לתוצאה 13 ולאחר מכן לוקחים את השארית מחלוקה ב 26.
כך ש $a \oplus a = (0+0+13)\%26 = 13 = n$, $r \oplus q = (17+16+13)\%26 = 20 = u$, וכאשר אליס ובוב אומרים במקביל hello/world מתקבל:

h	b	e	b	l	b	l	b	o	b
7	1	4	1	11	1	11	1	14	1
a	w	a	o	a	r	a	l	a	d
0	22	0	14	0	17	0	11	0	3
20	10	17	2	24	5	24	25	1	17
u	**k**	**r**	**c**	**y**	**f**	**y**	**z**	**b**	**r**

סעיף א:
בקובץ עם הקלטים האישיים לתרגיל מופיע מה שגדי שמע. נסו לשחזר מה אמרו אליס ובוב.

סעיף ב:
כשאליס ובוב שמעו שגדי הצליח לשחזר את מה שהם אמרו הם החליטו להתחכם, וכל אחד מהם בחר אות אקראית אחת אשר החליפה את האות המקורית בה השתמש בשפת הסתרים (כלומר את האות a אצל אליס, והאות b אצל בוב). אם אליס בחרה את האות x, אז בכל מקום בו השתמשה בין אותיות באות a בשפה המקורית, היא תשתמש עכשיו באות x. הם עדיין דיברו ביחד, וגדי שמע את החיבור של דבריהם. עיזרו לגדי לשחזר את דברי אליס ובוב.

שאלה 2:

מערכות הצפנה מסויימות מבוססות על השיטה הבאה. ישנו מפתח סודי x, ומי שיודע אותו יכול לפענח הודעות. (אנחנו רוצים שיכולת הפענוח תהיה מוגבלת רק לבעלי המפתח, ולא לאף אחד אחר.)

כחלק מהמערכת, ישנם מספרים שלמים g, p אשר ידועים לכל. כמו כן, ידוע לכולם מספר שלם y, אשר מחושב בצורה הבאה:

$y = g^x$ modulo p

לדוגמא, אם p=7, g=2, x=5 אז $y = 2^5$ modulo 7 = 4

במערכות אמיתיות, המודולוס p גדול מאד, וכך גם המפתח הסודי x.

תוקפי המערכת יודעים את הערכים g, p, $y=g^x$ modulo p , אך אינם יודעים את x. מטרתם היא למצוא את x.

בחידה שנציג לכם, x יהיה מספר שלם שנבחר באופן רנדומלי בתחום בין 0 ל 10^{12}.

הפרמטרים של המערכת: p=11333555557777777, g=123456789, את y תמצאו בקובץ הקלטים האישיים

אלגוריתם טריוויאלי שמקבל את g,p,y ומחפש את x יעבור על כל המספרים i בתחום בין 0 ל 10^{12}, ולכל אחד יבדוק אם g^i modulo p = y. זמן הריצה של אלגוריתם זה יהיה ארוך מידי ולא יספיק לפתרון החידה בזמן.

להלן תיאור של אלגוריתם יעיל יותר, אשר משתמש ב 10^6 יחידות זכרון, ומסיים לרוץ תוך 10^6 חישובים לכל היותר. עליכם לממש אלגוריתם זה ולפתור את החידה, כלומר למצוא את x.

האלגוריתם יעבוד בצורה הבאה:

קלט: g, p, y

פעולה:

1. חשב step = $g^{1,000,000}$ modulo p
2. צור מערך A ובו 10^6 מקומות. התא A[i] יכיל את הערך $step^i$ modulo p.
3. אם y שווה לאחד מהאיברים ב A, אז מצאנו את x. כלומר, אם y=A[i] אז x=1,000,000*i. (שימו לב שאולי כדאי לממש את A כמילון או טבלת hash בשביל לבצע בדיקה זו במהירות.)
4. נציב j=1
5. נחשב y = y*g modulo p
6. אם y שווה לאחד מהאיברים ב A, אז מצאנו את x. כלומר, אם y=A[i] אז x=1,000,000*i - j.
7. אחרת, נציב j=j+1 ונחזור לשלב 5
8. נוציא את x כפלט

מדוע האלגוריתם עובד? שלב 2 בו נוצר המערך מציב ב A את הערכים ... ,$g^{3*1000000}$,$g^{2*1000000}$,$g^{1000000}$

כלומר, ערכים בהם החזקות מרוחקות זו מזו במרחק 1,000,000 .

בלולאה (שלבים 5-7), מחפשים מהו הערך j כך ש $y*g^j$ נמצא בטבלה. מכיוון שהמרחק בין זוג מקומות עוקבים בטבלה הוא 1,000,000 כפלים ב g, נצטרך להתקדם לכל היותר 1,000,000 בדיקות עד שנמצא את j הזה. כשנמצא אותו, קל לשחזר את הערך של x, כי x+j שווה לחזקה של האיבר שמצאנו בטבלה.

הזינו בטופס את ערכו של x