

שבילים למצוינות לכיתה ז' - חלק 2

הצפנה ופענוח

מדריך למורה

א. צופן הסטה

1. בכותרת כתוב "הצפנה ופענוח".
2. המסר המפוענח הוא "המילה הלועזית להצפנה היא קריפטוגרפיה".
 - שימו לב שכאשר מצפינים בצופן הסטה במקום 1, האות א הופכת ל-ב, אך כאשר מפענחים האות ב הופכת ל-א. לכן, למשל, האות הראשונה במסר המוצפן, "ו", הופכת לאות ה במסר המפוענח.
3. המסר המוצפן הוא "זעפלים להלץ זנלנז דירחב".
4. המסר המפוענח הוא "על ההתנקשות בי כתב שייקספיר את השורה המפורסמת – הגם אתה, ברוטוס?"
 - בחוברת זו בחרנו שלא להבדיל בין אותיות סופיות ואותיות רגילות. בהסטה במקום אחד, למשל, הפכנו את האות כ ל-ל, וגם את האות ך הפכנו ל-ל. את האות י הפכנו ל-כ כאשר ההחלפה היתה בתחילת מילה או באמצעה, ול-ך כאשר ההחלפה היתה בסוף מילה.
 - אפשר לזהות את הבחירה באמצעות הדוגמה הראשונה – חיל הרגלים מוכן לפעולה. כאשר הסטנו את המסר בשני מקומות, האות ל בסוף "חיל" הפכה לאות ן. בנוסף, האות ם בסוף "רגלים" הפכה לאות ס.
5. המסר המפוענח הוא "מצרים מתכוונת לתקוף בעוד יומיים".
האתגר בשאלה הוא שהמפתח אינו נתון. עלינו לנסות את ההסטות השונות ולגלות שהמסר הוצפן בהסטה של 4 מקומות.
6. כיוון שיש 22 אותיות בעברית, מסר המוצפן בהסטה של 22 מקומות לא יוסט כלל. הסטה ב-23 מקומות זהה להצפנה במקום 1.
שימו לב שניתן לדבר גם על הסטות לכיוון ההפוך, כלומר הסטה במספרים שליליים. כך, למשל, הסטה ב-5 זהה להסטה ב-17.
7. כיוון שהסטה ב-22 מקומות זהה למסר המקורי, קיימים 21 מפתחות הסטה אפשריים בלבד. עבור מסר שהוצפן בצופן הסטה, בדיקת כל 21 המפתחות תוביל בוודאות לפענוח הצופן.

8. א. המסר המפוענח הוא "ספר הודי עתיק מציין את ההצפנה בעל פה ובכתב כשתיים משישים וארבע האמנויות שכל גבר ואישה בני-תרבות חייבים לדעת".
הספר, אגב, הוא הקאמה סוטרה.
ב. המסר הוצפן לפי מפתח 7, ולכן זה מספר המפתחות שהיה עלינו לבדוק.
ג. אין צורך לבדוק כל פעם את כל המסר. המילה הראשונה לרוב תספיק לנו בכדי לדעת אם המפתח הנבדק מוביל אותנו למילים בעלות משמעות או לא. לעתים נאלץ לבדוק גם מילה נוספת. אם שתי המילים המפוענחות הראשונות הן בעלות משמעות, קרוב לוודאי שאנחנו במפתח הנכון.

9. א. האות השכיחה ביותר בקטע היא ו.
ב. האותיות ג, ז, ס ו-ק לא מופיעות בקטע בכלל.
ג. האות ו מופיעה 10 פעמים בתחילת מילה. הסיבה לכך שהיא נפוצה היא כמובן השימוש ב-ו החיבור. מטרת הסעיף היא להראות שאין להסתמך בלעדית על היישומן, וצריך לחשוב על כיוונים נוספים שיעזרו לנו בפענוח.
ד. המילה "את" היא מילת קישור נפוצה שחוזרת על עצמה בקטע זה ובאחרים, והמילה "אלוהים" חוזרת על עצמה בקטע שכן הוא לקוח מהתורה.
ה. השערות אפשריות:
• בקטע חדשותי פוליטי עשויות לחזור מילים כגון "כנסת", "שר", "חוק" ועוד.
• מילות קישור אחרות כגון "אל", "של", "על", עשויות להופיע לעתים קרובות.
• ה הידיעה עשויה להופיע לעתים קרובות בתחילת מילה.
וכמובן שישנן השערות אפשריות רבות נוספות.

10. א. מכיוון שהאות הראשונה במסר המקורי היא ב (בראשית), והאות הראשונה במסר המוצפן היא ד, המסר הוצפן לפי מפתח 2.
ב. ראינו בשאלה 9 סעיף א שהאות הנפוצה ביותר בקטע המקורי היא ו. אם כך, בהסטה לפי מפתח 2 כל ו תהפוך ל-ח, והיא תהיה האות הנפוצה ביותר במסר המוצפן.

11. בעזרת היישומן נגלה שהאות י מופיעה 21 פעמים בקטע, והאות ט מופיעה פעם 1 בלבד. אם כן, מצד אחד הספירה אינה דומה לתגלית החוקרים, שכן היחס אינו זהה, אך מהצד השני האות י באמת נפוצה הרבה יותר מאשר האות ט, גם אצל החוקרים וגם בקטע מ"בראשית". בקטע נתון, במיוחד באורך קצר יחסית, נוכל לצפות שהאות י אכן תהיה נפוצה מ-ט ברוב המקרים, אך היחס לא יהיה קבוע.

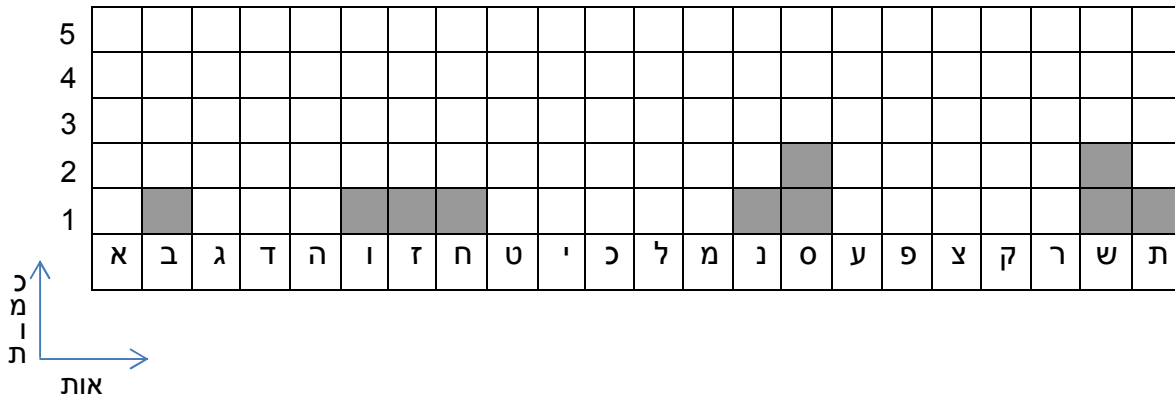
12. מטרת השאלה היא לחזור מעט על קריאת גרפים פשוטים, הבנת הצירים והעמודות, לפני שאנו מתקדמים לקריאת גרפים מסובכים יותר.
א. האות י הופיעה יותר פעמים מאשר האות ח בקטע אותו בדקו החוקרים.
ב. האות ז הופיעה כאלף פעמים בלבד בקטע אותו בדקו החוקרים, ויחד עם האות ט, היא האות הנדירה ביותר.

13. בקשו מהתלמידים להעתיק קטע באורך של 4-5 פסקאות לפחות, על מנת לראות את הדמיון בין גרף התפלגות האותיות במסר וגרף ההתפלגות בשפה.

התשובות לסעיפים א-ו הן בהתאם לקטע הנבחר. מטרת השאלות ליצור אצל התלמיד חוש אינטואיטיבי למידת הדמיון בין שני הגרפים.
ז. כדאי לעבוד עם קטעים החל ממילים בודדות ועד מספר עמודים. כמובן, נוכל לצפות שככל שהקטע ארוך יותר, מידת ההתאמה לגרף ההתפלגות בשפה תהיה גבוהה יותר. החל מגודל של עמוד או שניים, הגרפים יהיו דומים מאוד והגדלת הקטע לא תורגש.
ח. סוגים שונים של טקסט מתפלגים בצורות שונות זו מזו. הדבר בא לידי ביטוי בצורה בולטת במעבר מטקסט בכתב מלא לטקסט בכתב חסר. מפענחי צפנים נוהגים להשתמש בגרפים של התפלגות לשפה לפי סוג הטקסט אותו הם מנסים לפענח. כך, אם בחיל הים משתמשים בראשי-תיבות אופייניים, וחוזרים על מילים מסויימות (ים, ספינה...), נוכל לצפות להתפלגות שונה מההתפלגות בספר פרוזה. עם זאת, ההתפלגויות השונות בעברית עדיין יהיו דומות במידה מסויימת. למשל, סביר להניח שבכל סוג טקסט האות י תהיה נפוצה יותר מאשר האות ג.

14. א. כדי להראות את הדמיון בין התפלגות האותיות בשפה והתפלגות האותיות בקטע אקראי. רק בקטע ארוך מספיק דמיון זה ניכר.
ב. ככל שהקטע ארוך יותר, סביר להניח שהתפלגות האותיות בו תתכנס להתפלגות האותיות בשפה העברית.

15. א. בסידור אלפביתי של הציר האופקי, הגרף המוצפן מוסט ימינה לעומת הגרף המקורי, במספר מקומות הזהה למפתח ההסטה.
ב. הגרף של מסר מוצפן יוזז שמאלה כאשר נפענח אותו, שוב במספר מקומות הזהה למפתח לפיו נפענח.
ג. ראינו שבסידור אלפביתי הגרפים דומים אך מוסטים.
בסידור "לפי השכיחות במסר" הגרפים יראו זהים לחלוטין, אך הצירים האופקיים יהיו שונים (לגמרי, הצירים לא מוסטים אלא "מעורבים").
בסידור "לפי השכיחות בשפה" הגרפים שונים למדי - אמנם העמודות עצמן זהות (אם קיימת בגרף המקורי עמודה בגובה 30, תהיה עמודה כזו בוודאות גם בגרף של המסר המוצפן), אך הסדר שלהן אינו עונה על חוקיות מסויימת.



השוואת גרף זה לגרף השכיחות בשפה לא מאפשרת לנו לנחש את המפתח הנכון.
 ב. בהעדר ניחוש נאלץ לבדוק את המפתחות בזה אחר זה, ומכיוון שהמסר הוצפן לפי מפתח 9, זה מספר המפתחות שנבדוק. המסר המפוענח הוא "שרלוק הולמס".
 ג. קל יותר וכדאי לנסות לפענח מסר ארוך ככל שניתן, מכיוון שהתפלגות האותיות בו תהיה דומה יותר להתפלגות האותיות בשפה מאשר מסר קצר. בנוסף, בפענוח מסר ארוך יש סיכוי טוב יותר לגילוי "רמזים" נוספים, כפי שנראה בהמשך הפרק.
 ד. התשובה לשאלה זו נתונה במסגרת שמתחת לשאלה.

19. המסר הוצפן לפי מפתח 11.

המסר המפוענח הוא "לא קל לפענח קטע שחסר את מה שנמצא לאחר ה. כך גם ללא מה שנמצא לאחר ט. אפשר לסבך הצפנה בעזרת כתב חסר, למשל, לא רק בעזרת מסר קצר. רב הזמן גם את המלם החסרת אפשר לקרא ללא מאמץ!"

מטרת השאלה להראות דרך נוספת להקשות על פענוח צופן מלבד קיצורו. כדאי לעודד את התלמידים להמציא דרכים נוספות משל עצמם.

20. דרכים נוספות להקשות על פענוח מסר:

- הסרת הרווחים בין האותיות. שיטה זו תקשה על זיהוי המילים המפוענחות, אך לא תשנה את התפלגות האותיות במסר.
- הוספת אותיות לא נפוצות, למשל בסוף מילה: מסרפ זהג אפשריט לקריאהץ.
- שינוי השימוש בסופיות: למשל יצירת הסטה נפרדת לסופיות בלבד, כך שבהסטה לפי מפתח 1 תהפוך האות ך ל־ם, האות ם תהפוך ל־ן, ן ל־ף וכו'.

ב. צופן החלפה

1. המסר המוצפן הוא "קנרגק גפנק טידל".

2. המסר המפוענח הוא "צופן חלש גרם למותה של מרי מלכת הסקוטים".

על מרי מלכת הסקוטים תוכלו לקרוא כאן:

<http://he.wikipedia.org/wiki/%D7%9E%D7%A8%D7%99,%D7%9E%D7%9C%D7%9B%D7%AA%D7%94%D7%A1%D7%A7%D7%95%D7%98%D7%99%D7%9D>

מרי ניסתה למרוד במלכה אליזבת הראשונה בזמן שהותה בכלא, והעבירה מסרים מוצפנים לתומכיה. הצופן פוצח על ידי אנשיה של אליזבת ואלה שלחו למרי מכתב מוצפן המבקש את שמות כל המעורבים בניסיון המרד. כיוון שהמסר היה מוצפן, מרי לא חששה שהוא בעצם מאת אויביה. היא מסרה את שמות הקושרים, ואלו הוצאו להורג, יחד עם מרי עצמה. עוד על המקרה תוכלו לקרוא בספרו של סיימון סינג "סודות ההצפנה".

3. במסר המקורי, עבור מסר ארוך, הגרפים של ההתפלגות בשפה ובמסר אמורים להיות דומים זה לזה.

4. כאשר אנחנו מסדרים את שני הגרפים על פי שכיחות במסר, שני הגרפים יראו זהים לחלוטין, מלבד האותיות בציר האופקי.

5. כל צופן הסטה הוא צופן החלפה כיוון שצופן הסטה מקיים החלפה של אות באות ושמירה על חד-הערכיות, אך לא כל צופן החלפה הוא צופן הסטה, שכן לא כל צופן הסטה שומר על המרווח הקבוע בין האותיות השונות והסדר שלהן.

• הנביא התכוון לממלכת בבל

6. שלושת המפתחות הנותרים הם:

א ב ג
↓ ↓ ↓
ב א ג

א ב ג
↓ ↓ ↓
ב ג א

א ב ג
↓ ↓ ↓
ג ב א

7. 24 המפתחות עבור צופן בן 4 אותיות הם:

| | | | | | |
|---------|---------|---------|---------|---------|---------|
| א ב ג ד | א ב ג ד | א ב ג ד | א ב ג ד | א ב ג ד | א ב ג ד |
| ↓ ↓ ↓ ↓ | ↓ ↓ ↓ ↓ | ↓ ↓ ↓ ↓ | ↓ ↓ ↓ ↓ | ↓ ↓ ↓ ↓ | ↓ ↓ ↓ ↓ |
| ד ב א ג | ד ב ג א | ד ג ב א | ד א ב ג | ד א ג ב | ד ג א ב |

| | | | | | |
|---------|---------|---------|---------|---------|---------|
| א ב ג ד | א ב ג ד | א ב ג ד | א ב ג ד | א ב ג ד | א ב ג ד |
| ↓ ↓ ↓ ↓ | ↓ ↓ ↓ ↓ | ↓ ↓ ↓ ↓ | ↓ ↓ ↓ ↓ | ↓ ↓ ↓ ↓ | ↓ ↓ ↓ ↓ |
| ב ד א ג | ב ד ג א | ג ד ב א | א ד ב ג | א ד ג ב | ג ד א ב |

| | | | | | |
|---------|---------|---------|---------|---------|---------|
| א ב ג ד | א ב ג ד | א ב ג ד | א ב ג ד | א ב ג ד | א ב ג ד |
| ↓ ↓ ↓ ↓ | ↓ ↓ ↓ ↓ | ↓ ↓ ↓ ↓ | ↓ ↓ ↓ ↓ | ↓ ↓ ↓ ↓ | ↓ ↓ ↓ ↓ |
| ב א ד ג | ב ג ד א | ג ב ד א | א ב ד ג | א ג ד ב | ג א ד ב |

| | | | | | |
|---------|---------|---------|---------|---------|---------|
| א ב ג ד | א ב ג ד | א ב ג ד | א ב ג ד | א ב ג ד | א ב ג ד |
| ↓ ↓ ↓ ↓ | ↓ ↓ ↓ ↓ | ↓ ↓ ↓ ↓ | ↓ ↓ ↓ ↓ | ↓ ↓ ↓ ↓ | ↓ ↓ ↓ ↓ |
| ב א ג ד | ב ג א ד | ג א ב ד | א ב ג ד | א ג ב ד | ג א ב ד |

8. המשך הטבלה במשימה זו הוא לפי העצרות. בתא הריק הראשון התשובה היא 5!, כלומר 120.

9. א. אם נאמר שאדם 1 יכול לבדוק מפתח אחד בכל שניה אז:
 בכל דקה יבדוק 60 מפתחות.
 בכל שעה יבדוק 3600 מפתחות.
 בכל יום יבדוק 86400 מפתחות.
 בכל שנה יבדוק 31,536,000 מפתחות.
 ובסך הכל יקח לאדם 1,124,000,727,777,607,680,000 לחלק ב-31,536,000 מפתחות, שהם כ-30 טריליון שנים.
 כמובן שכל חישוב אחר עשוי להתאים גם כן.
 הערה: אפשר להדגיש שזהו הזמן שייקח לבדוק את כל המפתחות, כלומר זמן הבדיקה המקסימלי. בפועל, ייתכן שכבר המפתח הראשון יהיה נכון, אך הזמן המקסימלי הוא אינדיקציה לזמן שכנראה ייקח לפצח את הצופן, והוא באותו סדר גודל כמוהו.
 ב. 30 טריליון שנים הן כ-10 קוודריליון ימים (קוודריליון שווה 10^{15}).
 אם כן, יידרש מספר דומה של אנשים, בערך פי מיליון ממספר האנשים על פני כדור הארץ, על מנת לפענח את הצופן ביממה. כמובן שההערה מסעיף א תקפה גם כאן.

10. כפי שבחלק א במשימה 17 הצלחנו להפחית את מספר המפתחות שבדקנו מ-15 ל-2 באמצעות שימוש בסטטסטיקה, כך נוכל לעשות גם במקרה הזה. כמובן שהפעם המשמעות של קיצור הדרך תהיה משמעותית הרבה יותר – מעבר מהבלתי אפשרי אל האפשרי.

11. א. המילה "אמריקני" לא יכולה להיות המילה המקורית מכיוון שהאות הראשונה אינה זהה לאות הרביעית, והאות השניה אינה זהה לאות החמישית, כמו במילה המוצפנת.
ב. המילה "קונקורד" אכן מתאימה להיות המילה המקורית.
ג. הצעות למילים נוספות המתאימות לתבנית: פראפרזה, קאשקאבל, גרוגרת.

12. המסר המפוענח הוא: "לעתים קרובות קל לנחש מילים מסוימות."

13. המסר המפוענח הוא: "גם כאשר פותרים שאלה מתמטית, כדאי להשתמש בידע ובהגיון שלנו כדי להגיע לפתרון בצורה מהירה יותר!"

14. אין מחקרים רבים על שכיחות מילים בעברית.

רשימה של מילים נפוצות בעברית (יש להתייחס בערבון מוגבל):

http://www.lexiteria.com/word_frequency/hebrew_word_frequency_list.html

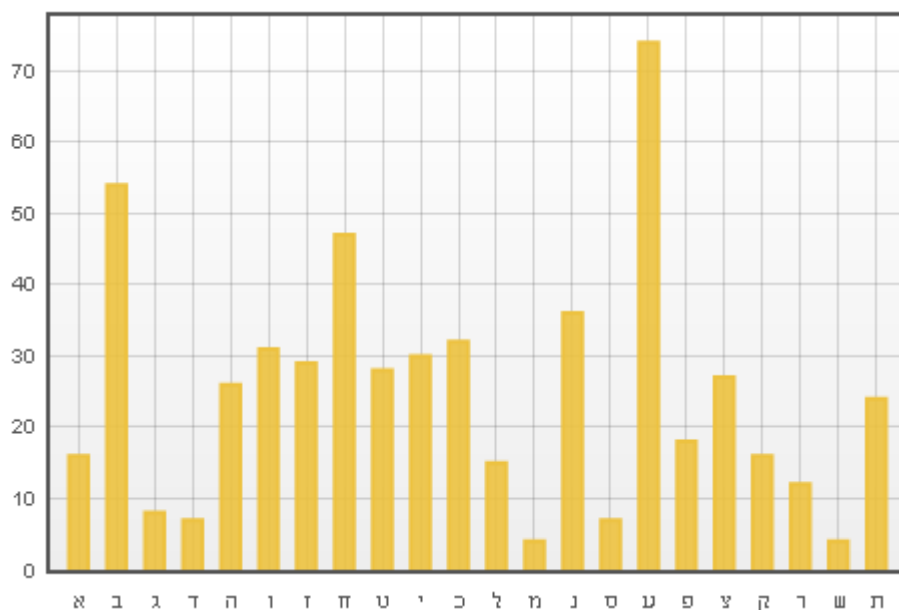
ככלל, מעבר לתבניות הנתונות במסגרת, נוכל לדבר גם על שכיחות רבה של אותיות בכל"ם בתחילת מילה (בשבוע הבא, כראוי, הלכתי לחנות, הוצאתי מהתנור).

אותיות שמופיעות לפני הסימן ' יהיו כנראה ג או ז (ג'ורג', ז'ורנל).

רעיונות לתבניות נוספות תוכלו למצוא בקישור הבא:

<http://scottbryce.com/cryptograms/stats.htm>

15. גרף השכיחויות של המסר המוצפן הוא:



16. א. האותיות השכיחות ביותר במסר המוצפן הן ע, ב, ח.
ב. האותיות הנדירות במסר המוצפן הן ש, מ, ד.
ג. סביר להניח שהן מייצגות את האותיות הנדירות בשפה: ז, ט, ג.

17. המסר המפוענח הוא:

"שיטת הפענוח בה הנכם משתמשים כרגע נקראת ניתוח תדירויות, או קריפטוגרפיה. השיטה הוצגה לראשונה על ידי פילוסוף, מתמטיקאי, מוזיקאי ורופא ערבי, אבו יוסוף אל-כינדי, שהתגורר בכופה שבעיראק של ימינו במאה התשיעית לספירה. אל-כינדי פרסם חיבור בשם "כתב יד על פענוח הודעות קריפטוגרפיות" בו הוא מסביר כי כדאי להחליף את האות השכיחה ביותר במסר המוצפן עם זו הנפוצה ביותר בשפה, ולהמשיך להחליף כך עד לאות הנדירה ביותר. אל-כינדי נחשב לאבי הפילוסופיה האיסלאמית. בין השאר, הוא תרגם מיוונית לערבית כתבים של אריסטו, היה חבר ב"בית החוכמה" שבבגדד ולקח חלק בתור הזהב של האיסלאם, שנמשך כחמש מאות שנה החל מסוף המילניום הראשון ועד לתחילת המילניום השני לספירה. בשיטתו של אל-כינדי נעזרים מצפינים ומפענחים עד ימינו."

18. בין הקשיים בפענוח המסר יש:

- אותיות שלא מתחלפות עם האותיות המתאימות בשפה.
- מילים שנראות הגיוניות ונכונות למרות שהן לא.
- שיחזור צעדים לאחר ניחוש שגוי (המשך עבודה עם ניחוש שגוי עשויה להוביל למבוי סתום)

19. על מנת להקשות את פענוח המסר ראינו שאפשר:

- לשלוח מסרים קצרים.
- להוריד אותיות נפוצות (למשל על ידי שימוש בכתיב חסר).
- הוספת אותיות (למשל דרך שילוב שפת ה־ב, כמו בשיר "אבניבי" בו מילות הפזמון "אבניבי אובהבב אובותבך" משמען "אני אוהב אותך".
- להוריד רווחים בין המילים.

כמובן שיש דרכים רבות נוספות להקשות על פענוח הצופן. מבחינה סטטיסטית נוכל לומר שאנחנו רוצים לשנות את גודל המדגם, או להטות אותו.

משימות לסיכום:

21. הגרף שהמוצפן מוסט ימינה לעומת גרף התפלגות האותיות בשפה. ניתן לראות שהגרף הראשון מוסט ב-7 מקומות לעומת הגרף השני. כך, האות השכיחה ביותר במסר המוצפן היא פ, ולכן סביר שהיא מייצגת הסטה של האות הנפוצה בשפה, י.
22. אנחנו יודעים שמדובר בצופן הסטה, אך איננו יודעים את המפתח והמסר עצמו קצר מאוד – בן מילה אחת בלבד. אם כך, אין ברירה אלא לבדוק את כל המפתחות האפשריים. המפתח היחיד שייתן לנו מקום מפגש הגיוני יהיה המפתח ה-21. פענוח לפיו יגלה שהשניים יפגשו ברומא.
23. המפקד לא פעל בחכמה. פיצול המסר הארוך למסרים קצרים יקשה על הפענוח של המסר. עדיף היה לו היה נותן את המסר הארוך כולו לכל אחד מ-40 המפענחים.
24. האות הנפוצה בעברית היא י, והאות הנדירה היא ז. בהסטה במפתח 7 תהפוך כל י ל-פ, ועל כן היא תהיה הנפוצה במסר המוצפן. וכל ז תהפוך ל-ג, ועל כן היא תהיה הנדירה במסר המוצפן.
25. אפשר לראות שהגרף השני אינו הסטה של הגרף הראשון, ולכן סביר להניח שמדובר בצופן החלפה. המפתח הסביר ביותר יחליף את האותיות לפי השכיחות שלהם:

| | | | | | |
|---------|----------|----------|----------|--------|------------------|
| ϕ | θ | Ω | ζ | Π | אות במסר המוצפן: |
| ↓ | ↓ | ↓ | ↓ | ↓ | |
| ζ | θ | Π | Ω | ϕ | אות במסר המקורי: |