**מבוא להצפנה – תרגיל 2**

נחפש קודם את אורך המפתח. נחשב את מספר ההתאמות כשמזיזים את הטקסט בשני מקומות ובשלושה מקומות:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  | 1 | 1 | 2 | 1 | 2 | 2 | 0 | 1 | 2 | 2 | 1 | 2 | 2 | 1 | 0 |
|  | 1 | 1 | 2 | 1 | 2 | 2 | 0 | 1 | 2 | 2 | 1 | 2 | 2 | 1 | 0 |  |  |
| 1 | 1 | 2 | 1 | 2 | 2 | 0 | 1 | 2 | 2 | 1 | 2 | 2 | 1 | 0 |  |  |  |

עבור שני מקומות יש 3 התאמות ועבור שלושה מקומות 7.

מספר ההתאמות הגדול יותר מסמן את אורך המפתח הסביר ביותר, לכן אורך המפתח הוא 3.

נחלק את ההודעה לבלוקים של 3 אותיות לפי:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 1 | 2 |  | 1 | 2 | 2 |  | 0 | 1 | 2 |  | 2 | 1 | 2 |  | 2 | 1 | 0 |

נחפש עכשיו את המפתח.

לפי הנתון, ווקטורי התדירות הם:

האותיות הראשונות של הבלוקים הם:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 2 |  | 2 |  | 2 |  | 2 |  | 0 |

יש לנו 5 אותיות ראשונות.

1 מתוכן היא האות 0.

0 מתוכן הן האות 1.

4 מתוכן הן האותיות 2.

לכן, ווקטור התדירויות יהיה:

נחשב כעת את המכפלות הסקלריות:

*הערך המקסימלי הוא עבור i=2 ולכן האות הראשונה של המפתח היא 2.*

האותיות השניות של הבלוקים הם:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 |  | 2 |  | 1 |  | 1 |  | 1 |

יש לנו 5 אותיות שניות.

0 מתוכן הן האות 0.

4 מתוכן הן האות 1.

1 מתוכן היא האותיות 2.

לכן, ווקטור התדירויות יהיה:

נחשב כעת את המכפלות הסקלריות:

*הערך המקסימלי הוא עבור i=1 ולכן האות השנייה של המפתח היא 1.*

האותיות השלישיות של הבלוקים הם:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 |  | 1 |  | 0 |  | 2 |  | 2 |

יש לנו 5 אותיות שניות.

1 מתוכן היא האות 0.

2 מתוכן הן האות 1.

2 מתוכן היא האותיות 2.

לכן, ווקטור התדירויות יהיה:

נחשב כעת את המכפלות הסקלריות:

*הערך המקסימלי הוא עבור i=1 ולכן האות השלישית של המפתח היא 1.*

מפתח הצפנה הוא:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1 |  | 1 |  | 2 |

ולכן מפתח הפענוח הוא:

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 2 |  | 2 |  | 1 | = | 1+1 |  | 1+1 |  | 2+2 |

ההודעה המוצפנת:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 1 | 2 |  | 1 | 2 | 2 |  | 0 | 1 | 2 |  | 2 | 1 | 2 |  | 2 | 1 | 0 |

פענוח של ההודעה:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 0 | 0 |  | 0 | 1 | 0 |  | 2 | 0 | 0 |  | 1 | 0 | 0 |  | 1 | 0 | 1 |

כדי למצוא את מטריצת המפתח, צריך לחלק את טקסט המקור לבלוקים של שתי אותיות ולמצוא שני בלוקים שאיתם ניתן לבנות מטריצה הפיכה, ז"א עם דטרנמיננטה זרה ל 26.

ניקח את הבלוקים ואת

ומקבלים את המטריצה כך ש- ולכן המטריצה P הפיכה.

נבנה עכשיו את המטריצה הבנויה מהבלוקים המוצפנים המתאימים:

ואת

ומקבלים את המטריצה .

תהי K מטריצת מפתח ההצפנה: .

*מטריצת הפענוח היא:*

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *1* | *1* | *0* | *0* | *0* | *1* | *1* | *1* | *1* | *0* | *0* | *0* | *1* |

*קיבלנו מחזור של 7.*

*אורך המחזור המקסימלי הוא: ולכן אורך המחזור אינו מקסימלי.*

*יש שלושה אפסים עוקבים ולכן אורך נוסחאת הנסיגה הוא לפחות 4.*

*אורך המחזור המקסימלי עבור נוסחת נסיגה באורך 4 הוא: ואורך נוסחת הנסיגה הוא לפחות 3.*

*:*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| *1* | *1* | *0* | *0* | *0* | *1* |

*משתמשים בסיביות*

*קיבלנו את הנוסחה - .*

*נבדוק אם הנוסחה יוצרת את הסדרה של המפתח:*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| *0* | *0* | *0* | *0* | *0* | *1* |

*בסדרת המפתח הסיביות האחרונות הן 1 ולא 0.*

*:*

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| *1* | *1* | *1* | *1* | *0* | *0* | *0* | *1* |

*משתמשים בסיביות*

*קיבלנו את הנוסחה - .*

*נבדוק אם הנוסחה יוצרת את הסדרה של המפתח:*

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| *1* | *1* | *0* | *1* | *0* | *0* | *0* | *1* |

*בסדרת המפתח הסיביות היא 1 ולא 0.*

*:*

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *0* | *0* | *1* | *1* | *1* | *1* | *0* | *0* | *0* | *1* |

*משתמשים בסיביות*

*קיבלנו את הנוסחה - .*

*נבדוק אם הנוסחה יוצרת את הסדרה של המפתח:*

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *1* | *1* | *0* | *1* | *1* | *1* | *0* | *0* | *0* | *1* |

*בסדרת המפתח הסיביות האחרונות הן 100 ולא 011.*

* *ולכן, אין סדרה באורך קטנה מ- 6 היוצרת את סדרת המפתח.*

*ההצפנה היא -*

*לכן, הפענוח הוא -*

*בוב קיבל את סדרת הבלוקים: .*

*תהליך הפענוח של בוב:*

*אחרי הפענוח, בוב מקבל את ההודעה:*

*איב הקשיבה לתקשורת בין אליס לבוב.*

*לכן, איב יודעת את סדרת הבלוקים: בנוסף איב יודעת את . ואת המפתח .*

*בנוסף לאיב יש גם סדרת הבלוקים שנייה שנשלחה בין אליס לבוב: .*

*נראה אין איב מצליחה לפענח את סדרת הבלוקים השנייה שנשלחה.*

*ראשית, נראה איך היא יכולה לגלות את הבלוק ההתחלתי.*

*הפענוח הוא -*

*נציב:*

*וכך איב גילתה את הבלוק ההתחלתי (בגלל שהיא יודעת את , ו- ).*

*נראה כעת את הדרך שבה איב מפענחת את סדרת הבלוקים השנייה: ( זה פענוח ו- ).*

*נתון - , ו- .*

*נצפין את ההודעה:*

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *1* | *1* | *0* | *0* |  | *0* | *0* | *1* | *0* |  | *1* | *1* | *0* | *1* |

|  |  |  |  |
| --- | --- | --- | --- |
| *1* | *0* | *0* | *1* |

*עם בלוק התחלתי*

*ההודעה המוצפנת היא:*

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *0* | *0* | *0* | *1* |  | *0* | *0* | *0* | *0* |  | *1* | *0* | *1* | *1* |