**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 |