שם: שחר אשר
ת.ז. 209305408

מבוא להצפנה – תרגיל 2

.1

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

0	1	2	2	1	2	2	1	0	2	2	1	2	1	1		
		0	1	2	2	1	2	2	1	0	2	2	1	2	1	1
			0	1	2	2	1	2	2	1	0	2	2	1	2	1	1

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:

0	1	2	2	1	2	2	1	0	2	2	1	2	1	1

נחפש עכשיו את המפתח.
לפי הנתון, ווקטורי התדירות A_i הם:

$$A_1 = [0.7, 0.2, 0.1]$$
$$A_2 = [0.1, 0.7, 0.2]$$
$$A_3 = [0.2,0.1,0.7]$$

שם: שחר אשר
ת.ז. 209305408

האותיות הראשונות של הבלוקים הם:

0 2 2 2 2

יש לנו 5 אותיות ראשונות.

1 מתוכן היא האות 0.

0 מתוכן הן האות 1.

4 מתוכן הן האותיות 2.

לכן, ווקטור התדירויות יהיה:

$$V_1 = [\frac{1}{5}, \frac{0}{5}, \frac{4}{5}] = [0.2, 0, 0.8]$$

נחשב כעת את המכפלות הסקלריות:

$$A_1 \cdot V_1 = [0.7, 0.2, 0.1] \cdot [0.2, 0, 0.8] = 0.22$$

$$A_2 \cdot V_1 = [0.1, 0.7, 0.2] \cdot [0.2, 0, 0.8] = 0.18$$

$$A_3 \cdot V_1 = [0.2, 0.1, 0.7] \cdot [0.2, 0, 0.8] = 0.6$$

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

שם: שחר אשר
ת.ז. 209305408

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:

$$V_2 = [\frac{0}{5}, \frac{4}{5}, \frac{1}{5}] = [0, 0.8, 0.2]$$

נחשב כעת את המכפלות הסקלריות:

$$A_1 \cdot V_2 = [0.7, 0.2, 0.1] \cdot [0, 0.8, 0.2] = 0.18$$

$$A_2 \cdot V_2 = [0.1, 0.7, 0.2] \cdot [0, 0.8, 0.2] = 0.6$$

$$A_3 \cdot V_2 = [0.2, 0.1, 0.7] \cdot [0, 0.8, 0.2] = 0.22$$

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

שם: שחר אשר
ת.ז. 209305408

האותיות השלישיות של הבלוקים הם:

2 2 0 1 1

יש לנו 5 אותיות שניות.

1 מתוכן היא האות 0.

2 מתוכן הן האות 1.

2 מתוכן היא האותיות 2.

לכן, ווקטור התדירויות יהיה:

$$V_2 = [\frac{1}{5}, \frac{2}{5}, \frac{2}{5}] = [0.2, 0.4, 0.4]$$

נחשב כעת את המכפלות הסקלריות:

$$A_1 \cdot V_3 = [0.7, 0.2, 0.1] \cdot [0.2, 0.4, 0.4] = 0.26$$

$$A_2 \cdot V_3 = [0.1, 0.7, 0.2] \cdot [0.2, 0.4, 0.4] = 0.38$$

$$A_3 \cdot V_3 = [0.2, 0.1, 0.7] \cdot [0.2, 0.4, 0.4] = 0.36$$

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

מפתח הצפנה הוא:

2 1 1

ולכן מפתח הפענוח הוא:

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

ההודעה המוצפנת:

0 1 2 2 1 2 2 1 0 2 2 1 2 1 1

פענוח של ההודעה:

1 0 1 0 0 1 0 0 2 0 1 0 0 0 0

שם: שחר אשר
ת.ז. 209305408

.2

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 $\begin{bmatrix} V \\ i \end{bmatrix} = \begin{bmatrix} 21 \\ 8 \end{bmatrix}$ ואת $\begin{bmatrix} c \\ t \end{bmatrix} = \begin{bmatrix} 2 \\ 19 \end{bmatrix}$

ומקבלים את המטריצה $P = \begin{bmatrix} 21 & 2 \\ 8 & 19 \end{bmatrix}$ כך ש- $\begin{vmatrix} 21 & 2 \\ 8 & 19 \end{vmatrix} = 19$ ולכן המטריצה P הפיכה.

נבנה עכשיו את המטריצה הבנויה מהבלוקים המוצפנים המתאימים:

$\begin{bmatrix} L \\ z \end{bmatrix} = \begin{bmatrix} 11 \\ 25 \end{bmatrix}$ ואת $\begin{bmatrix} l \\ g \end{bmatrix} = \begin{bmatrix} 11 \\ 6 \end{bmatrix}$

ומקבלים את המטריצה $Q = \begin{bmatrix} 11 & 11 \\ 25 & 6 \end{bmatrix}$.

תהי K מטריצת מפתח ההצפנה: $Q = KP \Longrightarrow K = QP^{-1}$.

$$P^{-1} = \frac{1}{17}\begin{bmatrix} 19 & -2 \\ -8 & 21 \end{bmatrix} = 23\begin{bmatrix} 19 & -2 \\ -8 & 21 \end{bmatrix} = \begin{bmatrix} 21 & 6 \\ 24 & 15 \end{bmatrix}$$

$$K = QP^{-1} = \begin{bmatrix} 11 & 11 \\ 25 & 6 \end{bmatrix}\begin{bmatrix} 21 & 6 \\ 24 & 15 \end{bmatrix} = \begin{bmatrix} 1 & 23 \\ 19 & 6 \end{bmatrix}$$

מטריצת הפענוח היא:

$$K^{-1} = \frac{1}{11}\begin{bmatrix} 6 & -23 \\ -19 & 1 \end{bmatrix} = 19\begin{bmatrix} 6 & -23 \\ -19 & 1 \end{bmatrix} = \begin{bmatrix} 10 & 5 \\ 3 & 19 \end{bmatrix}$$

שם: שחר אשר
ת.ז. 209305408

.3