

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	1
			0	1	2	2	1	2	2	1	0	2	2	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:

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

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

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

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:

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

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.

האותיות השניות של הבלוקים הם:

1 1 1 2 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:

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

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.

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:

$$2+2 \quad 1+1 \quad 1+1 \quad = \quad \boxed{1 \quad 2 \quad 2}$$

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