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:

$$A_0 = [0.7, 0.2, 0.1]$$
$$A_1 = [0.1, 0.7, 0.2]$$
$$A_2 = [0.2,0.1,0.7]$$

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:

$$A_0 \cdot V_1 = [0.7, 0.2, 0.1] \cdot [0.2, 0, 0.8] = 0.22$$

$$A_1 \cdot V_1 = [0.1, 0.7, 0.2] \cdot [0.2, 0, 0.8] = 0.18$$

$$A_2 \cdot V_1 = [0.2, 0.1, 0.7] \cdot [0.2, 0, 0.8] = 0.6$$

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:

$$A_0 \cdot V_2 = [0.7, 0.2, 0.1] \cdot [0, 0.8, 0.2] = 0.18$$

$$A_1 \cdot V_2 = [0.1, 0.7, 0.2] \cdot [0, 0.8, 0.2] = 0.6$$

$$A_2 \cdot V_2 = [0.2, 0.1, 0.7] \cdot [0, 0.8, 0.2] = 0.22$$

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:

$$A_0 \cdot V_3 = [0.7, 0.2, 0.1] \cdot [0.2, 0.4, 0.4] = 0.26$$

$$A_1 \cdot V_3 = [0.1, 0.7, 0.2] \cdot [0.2, 0.4, 0.4] = 0.38$$

$$A_2 \cdot V_3 = [0.2, 0.1, 0.7] \cdot [0.2, 0.4, 0.4] = 0.36$$

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

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:

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

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

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

$$P^{-1}=\frac{1}{19}\begin{bmatrix}19 & -2\\-8 & 21\end{bmatrix}=11\begin{bmatrix}19 & -2\\-8 & 21\end{bmatrix}=\begin{bmatrix}1 & 4\\16 & 23\end{bmatrix}$$

$$K=QP^{-1}=\begin{bmatrix}11 & 11\\25 & 6\end{bmatrix}\begin{bmatrix}1 & 4\\16 & 23\end{bmatrix}=\begin{bmatrix}5 & 11\\17 & 4\end{bmatrix}$$

מטריצת הפענוח היא:

$$K^{-1}=\frac{1}{15}\begin{bmatrix}4 & -11\\-17 & 5\end{bmatrix}=7\begin{bmatrix}4 & -11\\-17 & 5\end{bmatrix}=\begin{bmatrix}2 & 1\\11 & 9\end{bmatrix}$$

שם: שחר אשר
ת.ז. 209305408

.3

.a

1 0 0 0 1 1 1 1 0 0 0 1 1

קיבלנו מחזור של 7.
אורך המחזור המקסימלי הוא: $2^6 - 1 = 63$ ולכן אורך המחזור אינו מקסימלי.

.b

יש שלושה אפסים עוקבים ולכן אורך נוסחאת הנסיגה הוא לפחות 4.
אורך המחזור המקסימלי עבור נוסחת נסיגה באורך 4 הוא: $2^4 - 1 = 15$ ואורך נוסחת הנסיגה הוא לפחות 3.

$\underline{m = 3}$:

משתמשים בסיביות 1 0 0 0 1 1

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \begin{bmatrix} c_0 \\ c_1 \\ c_2 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} = \begin{cases} c_0 = 0 \\ c_2 = 1 \\ c_1 = 1 \end{cases}$$

קיבלנו את הנוסחה - $Z_{n+3} = Z_{n+1} \oplus Z_{n+2}$.
נבדוק אם הנוסחה יוצרת את הסדרה של המפתח:

1 0 0 0 <u>0</u> <u>0</u>

בסדרת המפתח הסיביות האחרונות הן 1 ולא 0.

$\underline{m = 4}$:

משתמשים בסיביות 1 0 0 0 1 1 1 1

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} \begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} =$$

$$= \begin{cases} c_0 = 1 \\ c_1 = 1 \\ c_2 = 1 \\ c_1 + c_3 = 1 \end{cases} = \begin{cases} c_0 = c_1 = c_2 = 1 \\ 1 + c_3 = 1 \end{cases} = \begin{cases} c_0 = c_1 = c_2 = 1 \\ c_3 = 0 \end{cases}$$

קיבלנו את הנוסחה - $Z_{n+4} = Z_n \oplus Z_{n+1} \oplus Z_{n+2}$.
נבדוק אם הנוסחה יוצרת את הסדרה של המפתח:

1 0 0 0 1 <u>0</u> 1 1

בסדרת המפתח הסיביות היא 1 ולא 0.

שם: שחר אשר
ת.ז. 209305408

$\underline{m = 5}$:

משתמשים בסיביות 1 0 0 0 1 1 1 1 0 0

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \end{pmatrix} \begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \\ c_4 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} =$$

$$= \begin{cases} c_0 + c_4 = 1 \\ c_3 = 1 \\ c_2 + c_4 = 1 \\ c_1 + c_3 = 0 \\ c_0 + c_2 + c_4 = 0 \end{cases} = \begin{cases} c_0 + c_4 = 1 \\ c_3 = 1 \\ c_2 + c_4 = 1 \\ c_1 + 1 = 0 \\ c_0 + 1 = 0 \end{cases} = \begin{cases} 1 + c_4 = 1 \\ c_3 = c_1 = c_0 = 1 = \\ c_2 + c_4 = 1 \end{cases}$$

$$= \begin{cases} c_4 = 0 \\ c_3 = c_1 = c_0 = 1 = \\ c_2 + 0 = 1 \end{cases} = \begin{cases} c_4 = 0 \\ c_3 = c_1 = c_0 = c_2 = 1 \end{cases}$$

קיבלנו את הנוסחה - $Z_{n+5} = Z_n \oplus Z_{n+1} \oplus Z_{n+2} \oplus Z_{n+3}$.

נבדוק אם הנוסחה יוצרת את הסדרה של המפתח:

1 0 0 0 1 1 1 <u>0</u> <u>1</u> <u>1</u>

בסדרת המפתח הסיביות האחרונות הן 100 ולא 011.

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

שם: שחר אשר
ת.ז. 209305408

4.

a.

ההצפנה היא - $C_i = E_K(C_{i-1}) \oplus P_i$
לכן, הפענוח הוא - $P_i = E_K(C_{i-1}) \oplus C_i$

בוב קיבל את סדרת הבלוקים: $C_1C_2C_3C_3C_4C_5$.
נסמן את ה- C_3 הראשון כ- C_3 ואת השני כ- $C_3{}'$

תהליך הפענוח של בוב:

$$P_1 = E_K(C_0) \oplus C_1$$
$$P_2 = E_K(C_1) \oplus C_2$$
$$P_3 = E_K(C_2) \oplus C_3$$
$$P_4' = E_K(C_3) \oplus C_3'$$
$$P_5' = E_K(C_3{}') \oplus C_4$$
$$P_6 = E_K(C_4) \oplus C_5$$

אחרי הפענוח, בוב מקבל את ההודעה: $P_1P_2P_3P_4'P_5'P_6$

b.

איב הקשיבה לתקשורת בין אליס לבוב.
לכן, איב יודעת את סדרת הבלוקים: $C_1C_2C_3C_3C_4C_5$ בנוסף איב יודעת את $P_1P_2P_3$. ואת המפתח K .
בנוסף לאיב יש גם סדרת הבלוקים שנייה שנשלחה בין אליס לבוב: $Q_1Q_2Q_3 \cdots Q_n$.
נראה אין איב מצליחה לפענח את סדרת הבלוקים השנייה שנשלחה.

ראשית, נראה איך היא יכולה לגלות את הבלוק ההתחלתי.
הפענוח הוא - $P_i = E_K(C_{i-1}) \oplus C_i$

נציב:

$$P_1 = E_K(C_0) \oplus C_1$$
$$P_1 \oplus C_1 = E_K(C_0)$$
$$D_K(P_1 \oplus C_1) = C_0$$

וכך איב גילתה את הבלוק ההתחלתי C_0 (בגלל שהיא יודעת את C_1, E_K ו- P_1).

שם: שחר אשר
ת.ז. 209305408

נראה כעת את הדרך שבה איב מפענחת את סדרת הבלוקים השנייה: (T_i זה פענוח Q_i ו- $C_0 = Q_0$).

$$
\begin{aligned}
T_1 &= E_K(Q_0) \oplus Q_1 \\
T_2 &= E_K(Q_1) \oplus Q_2 \\
&\vdots \\
T_n &= E_K(Q_{n-1}) \oplus Q_n
\end{aligned}
$$

.c

נתון - $m = 4$, ו- $E_K(abcd) = abcd \oplus 1111$.

נצפין את ההודעה:

1 0 1 1 0 1 0 0 0 0 1 1

עם בלוק התחלתי $X =$ 1 0 0 1

$$
\begin{aligned}
(1001 \oplus 1111) \oplus 1011 &= 1101 \\
(1011 \oplus 1111) \oplus 0100 &= 0000 \\
(0100 \oplus 1111) \oplus 0011 &= 1000
\end{aligned}
$$

ההודעה המוצפנת היא:

1 1 0 1 0 0 0 0 1 0 0 0