תרגיל בית 2

הנחיות:

- הגשה ב**בודדים**. עליכם לכתוב את הפתרונות לבד ולהגיש ביחידים.
- קראו את השאלות בעיון לפני שתתחילו בפתרונן.
- הקפידו לתעד את הקוד שלכם בהערות באנגלית.
- מלבד מילואים, לא יתקבלו תרגילים אחרי מועד הגשה. הגשה באיחור לאחר מועד הגשה נחשבת כאי-הגשה.
- כל יום מילואים = יום דחייה. על מנת לקבל את הדחייה, עליכם לשלוח באי-מייל למתרגל האחראי על תרגיל זה עותק של האישור המראה שהייתם במילואים (טופס 3010). אם האישור יגיע אליכם בתאריך מאוחר, יש להודיע על כך למתרגל האחראי על התרגיל.
- **לא ניתן לערער על תוצאות הבדיקה האוטומטית.**
- **שימו לב! הבדיקה הינה אוטומטית, ולכן הקפידו להדפיס בדיוק בפורמט שהתבקשתם ובידקו עם אתר הבדיקה ועם DiffMerge את הפלט שלכם מול הפלט של הדוגמאות שקיבלתם.**
  - השתמשו ב-redirection כדי להפנות את הפלט לקובץ טקסט.
  - וודאו את האותיות הגדולות והקטנות לפי הדוגמאות וההסברים בתרגיל.
  - אין להדפיס רווחים שלא התבקשתם להדפיס (בתחילת שורה או בסופה).
- בתרגיל זה מותר להשתמש בפונקציות מהספרייה stdbool.h, stdlib.h, stdio.h למעט במקרים בהם נאמר אחרת. החומר הנדרש לתרגיל זה שייך לתרגולים 1-5. אין להשתמש בחומר שאינו מופיע במצגות אלה.
- ההגשה הינה אלקטרונית ו**בבודדים** דרך אתר הקורס. קובץ ההגשה יהיה מסוג **zip** (ולא אף פורמט אחר) ויכיל בתוכו את הקבצים הבאים בלבד, ללא כל תיקיות:
  - קובץ **students.txt** עם שמך **באנגלית**, מספר תעודת הזהות וכתובת האי-מייל שלך.
  - קובץ פתרון **hw2q1.c** עבור שאלה 1.
  - קובץ פתרון **hw2q2.c** עבור שאלה 2.
  - קובץ פתרון **hw2q3.c** עבור שאלה 3.
- **חובה לשמור את קוד אישור ההגשה שמקבלים מהמערכת לאחר שמגישים, עד לסיום הקורס.**
- יש להקפיד להגיש את כל הקבצים בדיוק עם השמות שמופיעים לעיל. הגשה שלא תעמוד בתנאי זה **לא תתקבל ע"י המערכת!** אם המערכת לא מקבלת את התרגיל שלכם, חפשו את הפתרון לבעיה באתר הקורס תחת הכפתור FAQ.
- קבועים בקוד:
  - יש להגדיר בעזרת #define כל קבוע משמעותי. שמות קבועים צריכים להיות באותיות גדולות בלבד, אם השם מכיל יותר ממילה אחת מילים יופרדו בעזרת מקף תחתון (למשל STUDENTS_NUM).
  - אין להשתמש בערכי ASCII ישירות. יש להשתמש בייצוג של התווים (למשל 'a').
- הזחות:
  - שיטת הזחה מקובלת – הזחת קוד בכל בלוק, למשל:

```
int main()
{
        // your code here
        while (…)
        {
                // your code here
```

```
        }
}
```

- אין להשתמש במשתנים גלובאליים או סטטיים.
- שמות משתנים/קבועים/פונקציות צריכים להיות אינפורמטיביים, להעיד על מטרתם.
- בהירות הקוד ותיעוד:
  - יש לתעד את הקוד באמצעות הערות באנגלית בלבד. במידה ויש כמה שורות קוד שניתן להסביר בקצרה מה המטרה שלהן, יש לשים הערה בהתחלה ואין צורך לתעד כל שורה.
  - יש לתעד פונקציות – לפני הפונקציה להוסיף הערה שמסבירה בקצרה מה הפונקציה עושה ומה המשמעות של הפרמטרים שלה.
  - התיעוד צריך להיות אינפורמטיבי, כלומר יש להסביר מה המטרה של שורות הקוד ולא לכתוב את הקוד במילים.
- אין לשכפל קוד שלא לצורך (למשל ריבוי קוד זהה במספר מקרי if-else שונים).
- אי-עמידה באחת מדרישות התרגיל תוביל לפגיעה בציון (שימוש בחומר שהיה אסור בתרגיל וכו').

באופן כללי – הקפידו על כתיבת קוד מסודר ומובן ככל שניתן תוך יישום העקרונות שנלמדו בכיתה.
מותר לכם לממש פונקציות עזר משלכם ולהשתמש בהן.

בונוס (10 נקודות לציון התרגיל):

יש לעמוד בדרישה הנ"ל:

- אורך כל פונקציה לא יעלה על 16 שורות קוד. הגבלה זו תקפה לכל הפונקציות, כולל main. רק שורות ריקות, שורות עם סוגר מסולסל בלבד, ושורות עם הערות בלבד לא נספרות. אסור לכתוב כמה פקודות שונות משמעותית באותה השורה, למשל כותרת תנאי\לולאה צריכה להיות בשורה נפרדת מגוף התנאי\לולאה.

שימו לב:

באתר הקורס פורסמו 3 קבצי שלד לשלושת השאלות בתרגיל תחת השמות :

- **hw2q1.c**
- **hw2q2.c**
- **hw2q3.c**

בקבצים אלו קיימות כבר פונקציות הדפסה (שהשמות שלהם מתחילים ב print) שבאמצעותם תדפיס התוכנית שלכם לפלט כמו שיפורט בהמשך בכל שאלה.
עליכם ליצור פרויקט לכל שאלה (לדוגמה פרויקט בשם **hw2q1** כפי שעשיתם בתרגילים הקודמים) ,אך להחליף את קובץ ה C שנוצר בפרויקט בקובץ המתאים לשאלה זו שפורסם באתר (לדוגמא **hw2q1.c** עבור פרויקט של שאלה 1).
אלו הם שלושת הקבצים שתגישו יחד עם קובץ **students.txt**.
בכל שאלה בתרגיל אתם יכולים להוסיף פונקציות עזר כרצונכם.

שאלה 1: אופרטורים לוגיים ואריתמטיים

במהלך השוד הגדול ביותר בהיסטוריה, של המטבעה המלכותית של ספרד, במטרה להדפיס 2.4 מיליארד אירו, נתקלו החבורה של הפרופסור בקשיים רבים.

לכן, החליט הפרופסור להכניס שחקני חיזוק נוספים לעזרת השודדים:

Walter_White, Daenerys_Targaryen, Doron_Kabilio.

הפרופסור מעוניין לנהל שוד הוגן, ולכן הוא שולח לכל היותר שחקן אחד פנימה. לשם כך, הוא זקוק לכם, כדי שתבנו לו תוכנה שתעזור לו לקבוע איזה מהם לשלוח!

המפקחת מוריליו, שמנסה לפענח את השוד, צריכה לנחש את שמו של הפרופסור בכדי להגיע אליו.

בחירת השחקן שיישלח פנימה נעשית על בסיס ניחוש המפקחת את שמו של הפרופסור באופן הבא:

1. אם ערכי ה-ASCII של האותיות המרכיבות את שמו של הפרופסור מהווה סדרה מונוטונית **עולה ממש** – Daenerys_Targaryen תישלח לקרב.
2. אם שמו של הפרופסור קצר מ-6 תווים **וגם** אינו מכיל את האות 'r' – Doron_Kabilio יישלח לקרב.
3. אם סכום ערכי ה-ASCII של האותיות המרכיבות את שמו של הפרופסור לא מתחלק ב-5 **או** אם שמו של הפרופסור עולה על 4 תווים - Walter_White יישלח לקרב.

כמו כן, במידה ובאפשרותו של הפרופסור לשלוח לשוד יותר משחקן אחד, יבחר הפרופסור לשלוח את הדמות הגדולה ביותר לקסיקוגרפית .

(Daenerys_Targaryen < Doron_Kabilio < Walter_White).

במידה ואף תנאי אינו מתקיים, הפרופסור לא ישלח אף שחקן פנימה.

עליכם לכתוב תוכנית הקולטת רצף תווים המסתיים בתו " ! " ומהווה את שם הפרופסור לדעתכם. על התוכנית להדפיס למסך את בחירתו של הפרופסור לפי ההנחיות בשאלה.

שאלה 2: מערכים חד מימדיים

באווירת הבחירות המקומיות לראשות העיר,
מטרתינו בשאלה זו היא לבחור נשיא חדש לטכניון!

המועמדים לתפקיד הם 13 המתרגלים בקורס.

כעת, תבחרו יחד עם שאר הסטודנטים בקורס את הנשיא החדש.

עליכם לכתוב תוכנית הקולטת מהמשתמש את הצבעות הסטודנטים בקורס "מבוא למדעי המחשב" עבור הנשיא החדש לטכניון.

כאמור, כל אחד מהמתרגלים מועמד לתפקיד זה, כאשר כל אחד מהם מיוצג ע"י מספר סידורי אחר:

- 1 – עדי 4 – דניאלה 7 – גסוב 10 – ניר 13 - יארה
- 2 – אלון 5 – דניאל 8 – עידו 11 - עומר
- 3 – אסף 6 – דימיטרי 9 – נג'יב 12 - יאיר

המשתמש יקליד לפי הסדר את ההצבעות של כל אחד מהסטודנטים, והתוכנית תדפיס היסטוגרמה (שתכיל עבור כל מועמד את מספר הסטודנטים שבחרו בו), ואת המתרגל שנבחר.

כמו כן, התוכנית קולטת מהמשתמש את התו באמצעותו תוצג ההיסטוגרמה.

שימו לב: אם קיימים 2 מתרגלים עם אותה כמות מצביעים, ייבחר זה שמיוצג ע"י מספר קטן יותר.

<u>לדוגמא</u>: אם אסף ונג'יב קיבלו את אותה כמות נקודות, אסף ייבחר (כי $3 < 9$).

<u>הערות למימוש</u>:

- יש לקלוט הצבעות עד לקבלת הערך 1- מהמשתמש (בפרט, מספר הסטודנטים אינו ידוע מראש, אך מובטח שהוא אינו חורג מטווח הייצוג של int).
- אין צורך לבדוק את תקינות הקלט בשאלה זו: ראשית, מתקבל תו כלשהו (ללא מגבלות). אח"כ, מתקבלים מספרים בטווח הרצוי, ונעצור כאשר מתקבל 1-. (יש להתעלם מתווים המגיעים אחריו!)
- המספרים שעל הציר האופקי מייצגים את המתרגלים. כל הצבעה של סטודנט מיוצגת ע"י התו הנבחר , הממוקם בעמודה המתאימה לניחושו.
  בדוגמה הראשונה למשל, ישנן 2 כוכביות מעל המתרגל 6 ,המייצגות 2 סטודנטים שהצביעו לו.
- האיות המדויק באנגלית של כל אחד מהמתרגלים לצורך הדפסת שמו מופיע <u>כאן</u>. את ההדפסה יש לבצע עם **ירידת שורה** בסוף.

דוגמאות הרצה:

```
Please enter a character:
*
Please enter votes:
5 6 6 7 7 7 8 8 8 8 9 9 9 10 10 11 -1
Histogram:
              *
            * * *
          * * * * *
        * * * * * *  *
1 2 3 4 5 6 7 8 9 10 11 12 13
Ido was elected!
```

```
Please enter a character:
@
Please enter votes:
7 7 7 7 8 8 8 9 9 10 11 11 12 12 12 13 13 13 13 -1
Histogram:
            @               @
            @ @         @   @
            @ @ @     @   @   @
            @ @ @ @   @   @   @
1 2 3 4 5 6 7 8 9 10 11 12 13
Gasob was elected!
```

```
Please enter a character:
O
Please enter votes:
1 8 7 3 9 10 13 5 2 12 11 4 6 -1
Histogram:
O O O O O O O O O O  O  O  O
1 2 3 4 5 6 7 8 9 10 11 12 13
Adi was elected!
```

דגשים להדפסת ההיסטוגרמה:

- יש להכניס רווח בין כל 2 עמודות (אך אין להכניס רווח לפני השורה הראשונה ואחרי השורה האחרונה). שימו לב כי עבור מתרגלים המיוצגים ע"י מספרים דו-ספרתיים יש להדפיס רווח נוסף.
- יש להדפיס בהתאם לפורמט המתואר בדוגמאות .

שאלה 3: לולאות מקוננות ומערכים דו – מימדיים

בשאלה זו, נמשיך לעזור לקיסר מתרגיל בית 1!

כזכור, בתרגיל הקודם הוא שלח לגנרלים שלו הוראות מוצפנות לשדה הקרב, אך לצערו האויבים הצליחו לפענח את כתב הסתר. הפעם, נבצע את ההצפנה בצורה יותר מתוחכמת!

נרצה כעת לממש צופן מוכר ששמו AES, שגם מטרתו היא לאפשר העברת מידע מסווג בין הקיסר ולוחמיו, כך שאף אחד אחר לא יוכל לפענח את המידע!

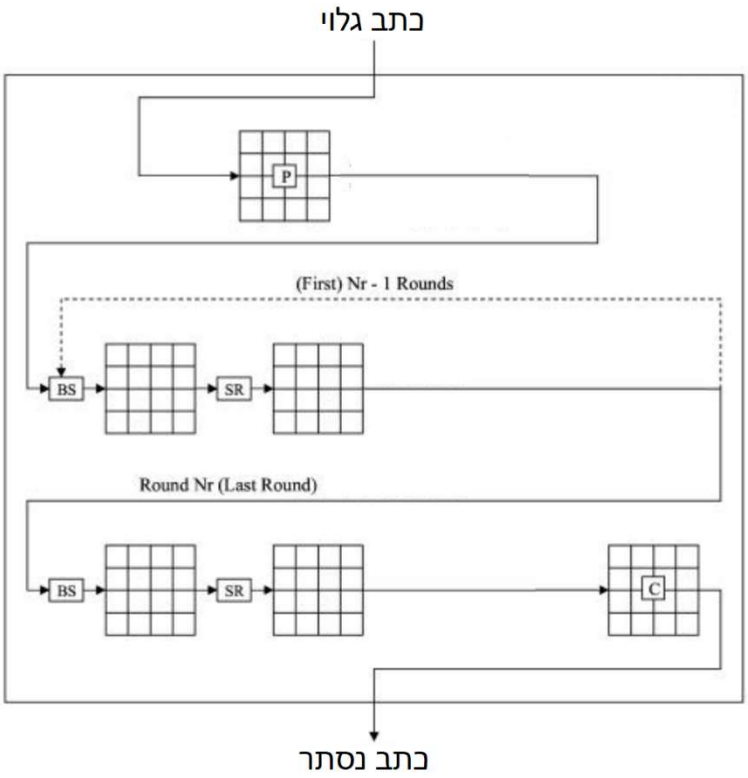
להקלתכם, נממש **רק חלק** מאלגוריתם AES, אשר עליו תוכלו לקרוא בהרחבה כאן (למי שמתעניין).

בתרגיל זה נממש רק את העברת המידע בצורת מאובטחת מהגנרל לחייליו (תהליך ההצפנה).

AES הוא אלגוריתם הצפנה שמקבל כקלט **2** פרמטרים:

- מפתח (ממנו **נתעלם** בתרגיל זה)
- הודעה שבה כל תו הוא **מספר שלם בין 0 ל-255** (כולל!), שמיוצג כמטריצה ריבועית (אורך ורוחב **זהים**), ופולט כתב סתר של ההודעה.

לצורך כך, נבצע 2 פעולות על המטריצה: Byte Substitution ו – Shift Rows, במשך מספר שלבים (Nr) אחד אחרי השני, באופן הבא:

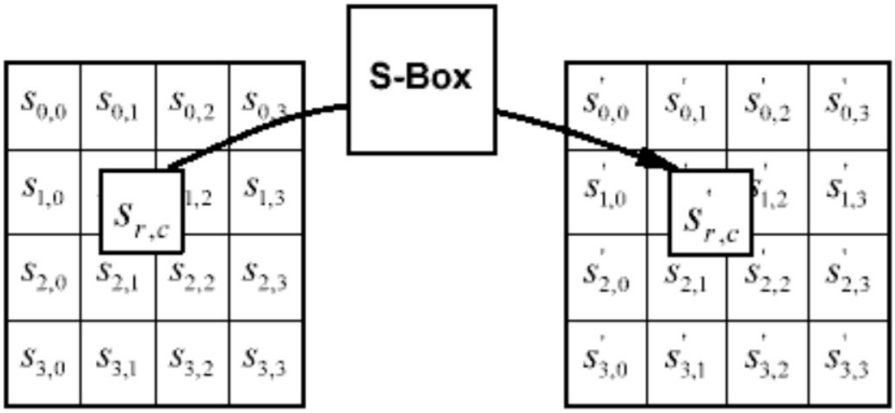


- החל מנקודה זו, בכל פעם שנכתוב מטריצה – נתייחס להודעה עצמה.

פעולה א' - Byte Substitution:

לרשותכם מצורף בקובץ hw2q3.c מערך ששמו s-box בגודל 256.

פעולה זו עובדת על בתים בודדים (כלומר על **כל** משבצת במטריצה בנפרד). בפעולה זו, נחליף כל ערך בערך אחר על סמך ה-s-box שהיא טבלת תרגום קבועה ומוגדרת מראש, <u>כך שהאיבר שערכו i יוחלף באיבר ה-i במקומו במערך</u>.



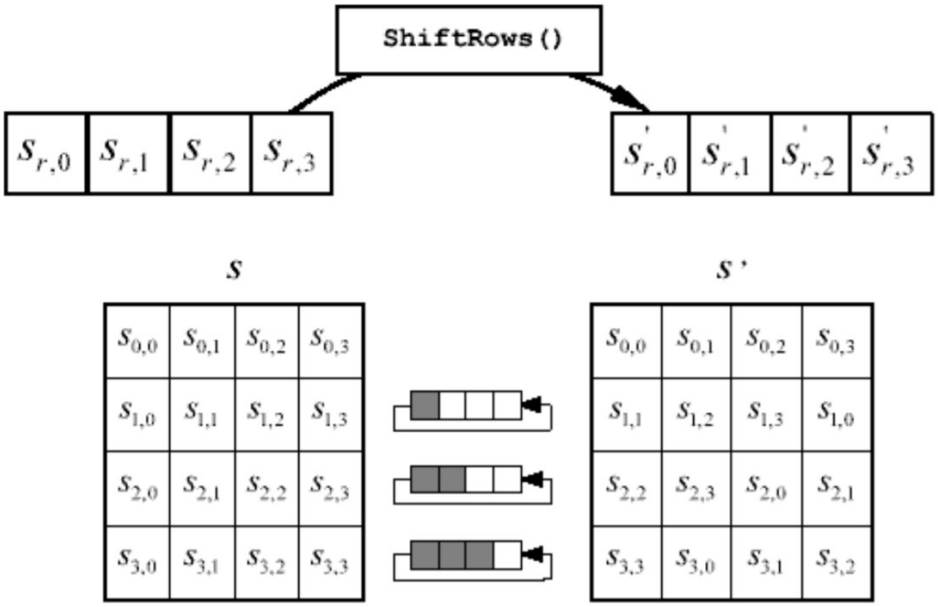
<u>לדוגמא</u>: את הערך 7 נחליף ב- sbox[7].

פעולה ב' – Shift Rows:

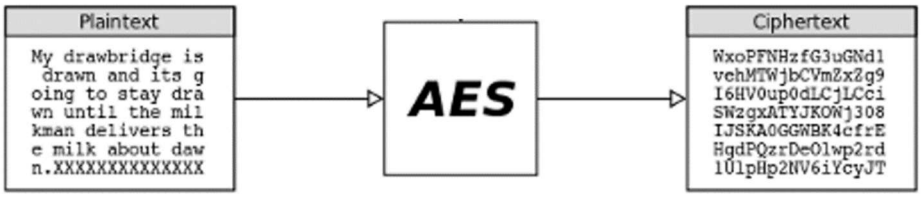
פעולה זו עובדת על שורות במטריצה.

באופן כללי מזיזים את השורה ה- i, כאשר $0 \le i \le n$, i מקומות שמאלה בצורה **מעגלית** (כאשר nxn הוא גודל המטריצה שהתקבל כקלט).

כלומר, שורה מספר אפס תישאר במקום, שורה מספר אחת תזוז מקום אחד שמאלה וכך הלאה.



הערה: שימו לב כי כל הפעולות שביצענו לצורך ההצפנה בגרסה מצומצמת זו של התרגיל, הינן הפיכות. לכן, אם נבצע את הפעולות ההפוכות בסדר הפוך, על כתב הסתר (טקסט מוצפן), נוכל לקבל את הכתב הגלוי . (אבל את זה לא נצטרך לממש בתרגיל זה ☺)



התוכנית תבצע לפי הסדר:

1. תבקש מהמשתמש להכניס את כמות האיטרציות בהן היא תבצע את הפעולות (**מספר שלם וגדול שווה לאפס**):

```
Starting the AES Algorithm, please pick amount of iterations:
```

2. אם מתקבל מספר שאינו עומד בתנאים, נדפיס שגיאה ונבקש קלט נוסף, עד שנקבל קלט מתאים:

```
Invalid amount of iterations!
Please try again:
```

3. לאחר מכן, נבקש את גודל המטריצה (ריבועית) שתכיל את ההודעה (מספר אחד שייצג גם את האורך וגם את הרוחב):

```
Please pick a matrix size:
```

4. כעת, נבקש שהמשתמש יקליד את המטריצה:

```
Please enter the matrix:
```

5. לבסוף, נבצע את ההצפנה, ככמות האיטרציות שנדרשו, ונפלוט את המטריצה שהתקבלה.
6. התוכנית תסיים את ריצתה בהצלחה.

דוגמאות הרצה:

```
Starting the AES Algorithm, please pick amount of iterations:
0
Please pick a matrix size:
3
Please enter the matrix:
1 2 3
4 5 6
7 8 9
The encrypted message is:
1 2 3
4 5 6
7 8 9
```

```
Starting the AES Algorithm, please pick amount of iterations:
5
Please pick a matrix size:
4
Please enter the matrix:
50 7 9 17
8 14 50 50
12 200 150 154
9 9 4 9
The encrypted message is:
69 5 116 22
145 69 69 167
81 237 23 45
116 116 116 74
```

```
Starting the AES Algorithm, please pick amount of iterations:
-1
Invalid amount of iterations!
Please try again:
1
Please pick a matrix size:
2
Please enter the matrix:
1 1
1 1
The encrypted message is:
124 124
124 124
```

בהצלחה!!!