



# **פרויקט גמר באסמבלי מדעי המחשב**

**מגיש: דניאל ריימן**

**מורה: שרה יחיאל**

**שנה: 2024**

**בית ספר: תיכון הראשונים**

**נושא: אלגוריתמים**

---

## תוכן עניינים

---

3	.....	תיאור פרויקט
5	.....	תרשים זרימה של התוכנית
6	.....	טבלת משתנים
8	.....	פעולות עיקריות
12	.....	קשיים ובעיות
13	.....	הערות
14	.....	רפלקציה אישית
15	.....	Alt Codes Reference Sheet

---

## תיאור פרויקט

---

### פרטים:

אלגוריתם: TEA Algorithm

שם: Cipher Command

שם קובץ התוכנית: ccommand.asm

### תיאור כללי:

התוכנית הזו היא תוכנית שנכתבה בשפת אסמבלי המיועדת למימוש אלגוריתם TEA האלגוריתם זה משמש להצפנת נתונים ופענוחם באופן מאובטח. התוכנית מתחילה עם תפריט המציע למשתמש לבחור בין הצפנה, פענוח או יציאה מהתוכנית. לאחר בחירת אפשרות, התוכנית מבקשת מהמשתמש להזין את המידע הנדרש - הודעה להצפנה או פענוח ומפתח סודי. לאחר הזנת המידע, התוכנית מבצעת את הפעולה הנבחרת, תוך הצפנת או פענוח המידע באמצעות אלגוריתם TEA לאחר מספר שניות ההודעה המוצפנת מוצגת על המסך, לבסוף התוכנית מחכה שהמשתמש ילחץ על מקש על למנת לחזור לתפריט הראשי.

### תיאור כללי של האלגוריתם:

- לקיחת טקסט, ומפתח מהמשתמש

○ גודל מקסימלי לטקסט ולמפתח:

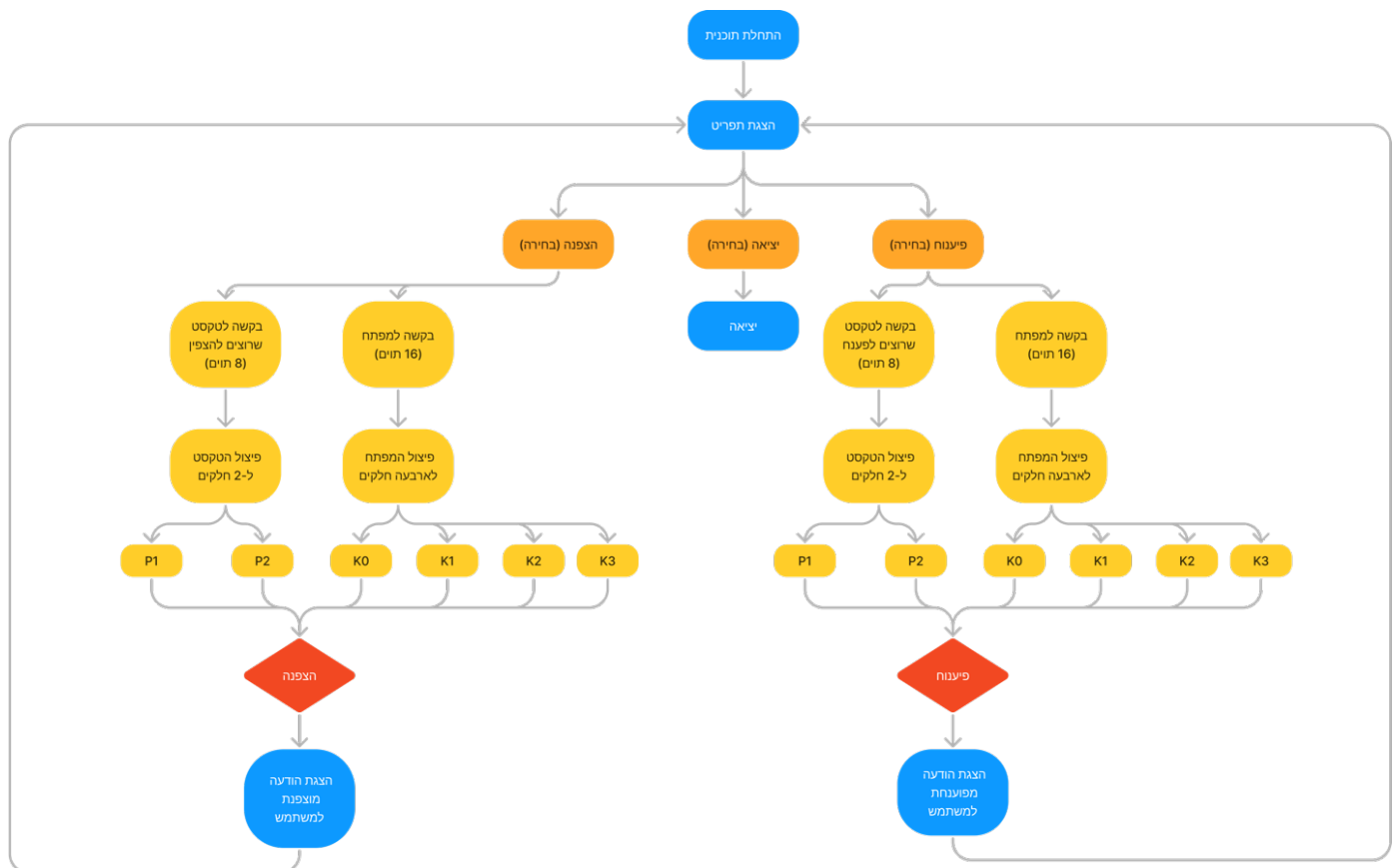
טקסט: 64 bits

מפתח: 128 bit

- חציית הטקסט לשני חלקים
- חציית המפתח לארבעה חלקים
- בתוך לולאה (מינימום 32 סיבובים) מבצעים פעולות של מיזוג בין הטקסט למפתח, עושים פעולות הוספה, הזזת ביטים, xor, וכו...
  - משתמשים בקבוע שנקרא delta עם הערך 9E3779B9 אשר מרחיב את חוזק ההצפנה.
- בסיום הלולאה של ה-32 סיבובים, ההודעה המוצפנת מוצגת.

## תרשים זרימה של התוכנית

תרשים זה הוא תרשים המתאר את תפקוד וביצוע התוכנית הכללית



**P1, P2** = The two parts of the plaintext

**K0, K1, K2, K3** = The four parts of the key

## טבלת משתנים

משתנה	תפקיד	גודל המשתנה
<b>headline</b>	תצוגת הכותרת הראשית של התוכנית.	-
<b>menu</b>	תפריט האפשרויות הראשי למשתמש.	-
<b>yourChoice</b>	תצוגת הבחירה של המשתמש.	-
<b>errorOptionMessage</b>	הודעת שגיאה במקרה שהמשתמש בוחר אפשרות לא חוקית.	-
<b>returnMenuPrompt</b>	הנחיה לחזור לתפריט לאחר בחירת אפשרות לא חוקית.	-
<b>encryptPlainTextPrompt</b>	הנחיה להזנת הטקסט שיש להצפין.	-
<b>encryptKeyPrompt</b>	הנחיה להזנת מפתח ההצפנה.	-
<b>decryptPlaintextPrompt</b>	הנחיה להזנת הטקסט שיש לפענח.	-
<b>decryptKeyPrompt</b>	הנחיה להזנת מפתח הפענוח (שווה למפתח ההצפנה).	-
<b>delta</b>	משתנה קבוע המשמש בהצפנה ובפענוח (ערך קבוע של TEA).	4 בתים
<b>sum</b>	משתנה עזר המשמש בחישובי ההצפנה והפענוח.	4 בתים
<b>plaintextBuffer</b>	זיכרון שמור לקלט הטקסט שהמשתמש מכניס להצפנה.	9 תווים

2 בתים	גודל זיכרון השמור לקלט הטקסט שהמשתמש מכניס להצפנה.	<b>plaintextBufferSize</b>
17 תווים	זיכרון שמור לקלט המפתח שהמשתמש מכניס להצפנה או פענוח.	<b>keyBuffer</b>
2 בתים	גודל זיכרון השמור לקלט המפתח שהמשתמש מכניס להצפנה או פענוח.	<b>keyBufferSize</b>
4 בתים כל אחד	חלקים של המפתח המפוצל המשמש בהצפנה ובפענוח.	<b>k0, k1, k2, k3</b>
4 בתים כל אחד	משתני פלט המשמשים להצפנה ופענוח של הטקסט.	<b>p1, p2</b>

---

## פעולות עיקריות

---

**:clearScreen**

קלט: אין.

פלט: אין.

תיאור: מנקה את המסך ומחזיר את סמן המסך למיקום ההתחלתי.

**:print**

קלט: value (מחרוזת להדפסה).

פלט: אין.

תיאור: מדפיס את המחרוזת הנתונה למסך.

**:inputNumber**

קלט: אין.

פלט: al (הערך המספרי המוקלד).

תיאור: מקבל קלט מספרי מהמשתמש וממיר אותו לערך מספרי.



### **:checkUserInput**

קלט: al (בחירת המשתמש).

פלט: אין.

תיאור: בודק את בחירת המשתמש ומעביר אותו לפרוצדורה המתאימה (הצפנה, פענוח, יציאה).

### **:userInputPlaintext**

קלט: אין.

פלט: plaintextBuffer (הטקסט המוזן).

תיאור: מקבל קלט מהמשתמש לטקסט המיועד להצפנה, ומאחסן אותו בזיכרון.

### **:userInputKey**

קלט: אין.

פלט: keyBuffer (המפתח המוזן).

תיאור: מקבל קלט מהמשתמש למפתח ההצפנה, ומאחסן אותו בזיכרון.

### **:encryptionSelection**

קלט: אין.

פלט: אין.

תיאור: מבצע את תהליך ההצפנה כולל קבלת הטקסט והמפתח מהמשתמש, הצפנת הטקסט והצגת התוצאה.

**:decryptionSelection**

קלט: אין.

פלט: אין.

תיאור: מבצע את תהליך הפענוח כולל קבלת הטקסט והמפתח מהמשתמש, פענוח הטקסט והצגת התוצאה.

**:encrypt**

קלט:  $p1, p2, k0, k1, k2, k3$  (טקסט מוצפן ומפתח הצפנה).

פלט: אין.

תיאור: מבצע הצפנה של הטקסט באמצעות אלגוריתם TEA, על פי מפתח ההצפנה המוזן.

**:decrypt**

קלט:  $p1, p2, k0, k1, k2, k3$  (טקסט מוצפן ומפתח הצפנה).

פלט: אין.

תיאור: מבצע פענוח של הטקסט באמצעות האלגוריתם

---

## קשיים ובעיות

---

במהלך כתיבת הקוד נתקלתי בהרבה סוגים של בעיות שונות שיכולות להיות. הסוג הראשון הוא בעיות הבנה. זה נושא חדש בשבילי לגמרי, אף פעם לא כתבתי אלגוריתם, ובמיוחד לא הצפנה, לכן היה לי ברור מההתחלה שאיתקל בבעיות כאלה.

אחרי שלמדתי והבנתי את הבסיס בקריפטוגרפיה ואת אופן הפעולה של הצפנה ופענוח, התחלתי לכתוב את הקוד. כאן הגיעה הבעיה השנייה – באגים. ידוע שקשה מאוד לדבאג בשפת אסמבלי, במיוחד בגלל שזו שפה ברמת המחשב הנמוכה וגם בגלל שאין הרבה חומר באינטרנט.

כמובן שלאחר זמן של ניסיונות מצאתי את הבאגים שהיו והכל רץ כרגיל. הבעיה השלישית שהייתה לי, ממש לקראת הסוף, היא שחשבתי שאני צריך להמיר בין סוגים כמו hex ל-ascii או להפך, ולא הבנתי שאין צורך להמיר כלום. המחשב ממיר את כל המידע להקס אוטומטית.

הבעיה האחרונה שלי הייתה איך לאפשר הכנסת הודעה מוצפנת באמצעות המקלדת. אז נזכרתי שיש כל מיני שילובי מקשים שיכולים ליצור סימנים של ascii. מצאתי דף עם שילובי מקשים לכל ערך ascii, וכך נפתרה הבעיה האחרונה שלי.

---

## הערות

---

### הפענוח

- בשביל לכתוב את ההודעה המוצפנת בחלק של הפענוח, יש להשתמש בדף המצורף ה-Alt Codes Reference Sheet. בדף זה נמצאים השילובים הנכונים של מקשים על מנת לכתוב סימנים באסקי שלא נמצאים במקלדת. לדוגמה, על מנת לכתוב  $\sqrt{\quad}$ , יש ללחוץ על Alt ובאותו הזמן להקיש במקש המספרי של המקלדת את 251, כלומר:

$$\text{Alt} + 251 = \sqrt{\quad}$$

---

## רפלקציה אישית

---

הפרויקט הזה היה קשה יותר ממה שמשחק היה אמור להיות מהסיבה שאף פעם לא למדנו משהו כמו אלגוריתמים והצפנות. לכן, היה לי יותר חומר ללמוד ולהבין מאשר כל מי שעשה משחק (לא שאני אומר שמשחק זה לא קשה ליצור). בנוסף, התהליך דרש ממני להתמודד עם בעיות חדשות ולא מוכרות.

כמו כן, הכתיבה בשפת אסמבלי הוסיפה לרמת הקושי. בניגוד לשפות תכנות אחרות, אסמבלי דורשת רמת דיוק גבוהה ותשומת לב לפרטים הקטנים ביותר. כל טעות קטנה יכולה לגרום לבאגים שקשה מאוד למצוא ולתקן.

עם הזמן והמאמץ שהשקעתי בפרויקט, למדתי הרבה על הצפנה. נאלצתי להיות סבלני שעם הזמן אני אגלה פתרון, ולמדתי כיצד לגשת לבעיות מורכבות בשלבים.

# ALT CODES REFERENCE SHEET

Hold down the "Alt" key then enter the code on the numeric keypad with Num Lock on

IM	Numbers	Greek	Currency	?s and !s	Letters with Accents	
Alt 1 ☉	Alt 48 - 57 0 - 9	Alt 224 α	Alt 0164 ₪	Alt 33 !	<b>Uppercase</b>	<b>Lowercase</b>
Alt 2 ☪	<b>Basic Operators</b>	Alt 225 β	Alt 156 £	Alt 19 !!	Alt 0192 À	Alt 0224 à
Alt 3 ♥	Alt 43 +	Alt 226 Γ	Alt 0128 €	Alt 173 ¡	Alt 0193 Á	Alt 0225 á
Alt 11 ♂	Alt 45 -	Alt 235 δ	Alt 36 \$	Alt 63 ?	Alt 0194 Â	Alt 0226 â
Alt 12 ♀	Alt 0215 ×	Alt 238 ε	Alt 155 ¢	Alt 168 ¿	Alt 0195 Ã	Alt 0227 ã
Alt 13 ♪	Alt 0247 ÷	Alt 233 Θ	Alt 157 ¥	<b>Brackets</b>	Alt 0196 Ä	Alt 0228 ä
Alt 14 ♫	<b>Pers</b>	Alt 227 π	Alt 158 ₧	Alt 40 (	Alt 0199 Ç	Alt 0231 ç
Alt 0169 ©	Alt 37 %	Alt 230 μ	Alt 159 ₣	Alt 41 )	Alt 0200 È	Alt 0232 è
Alt 169 ®	Alt 0137 ‰	Alt 228 Σ	<b>Accents</b>	Alt 91 [	Alt 0201 É	Alt 0233 é
Alt 0153 ™	<b>Bracketing</b>	Alt 229 σ	Alt 0180 `	Alt 93 ]	Alt 0202 Ê	Alt 0234 ê
<b>Filled Arrows</b>	<b>Alt Code Symbol</b>	Alt 231 τ	Alt 0184 ´	Alt 123 {	Alt 0203 Ë	Alt 0235 ë
Alt 16 ►	Alt 40 (	Alt 232 Φ		Alt 125 }	Alt 0204 Ì	Alt 0236 ì
Alt 17 ◄	Alt 41 )	Alt 237 φ		<b>Editing</b>	Alt 0205 Í	Alt 0237 í
Alt 254 ▣	<b>Plus or Minus</b>	Alt 234 Ω	<b>Drawing</b>	Alt 28 ¯	Alt 0206 Î	Alt 0238 î
Alt 30 ▲	Alt 241 ±	Alt 176 ☐	Alt 200 ▤	Alt 21 §	Alt 0207 Ï	Alt 0239 ï
Alt 31 ▼	<b>Fractions</b>	Alt 177 ☐	Alt 201 ▥	Alt 20 ¶	Alt 165 Ñ	Alt 164 ñ
<b>Line Arrows</b>	Alt 47 /	Alt 178 ☐	Alt 202 ▦	Alt 0134 †	Alt 0210 Ò	Alt 0242 ò
Alt 23 ↑	Alt 0188 ¼	Alt 179	Alt 203 ▧	Alt 0135 ‡	Alt 0211 Ó	Alt 0243 ó
Alt 24 ↑	Alt 0189 ½	Alt 180 ⊥	Alt 204 ▨	<b>Quotes</b>	Alt 0212 Ô	Alt 0244 ô
Alt 25 ↓	Alt 0190 ¾	Alt 181 ⊥	Alt 205 ▩	Alt 34 "	Alt 0213 Õ	Alt 0245 õ
Alt 26 →	Alt 46 .	Alt 182 ⊥	Alt 206 ▪	Alt 0139 ‹	Alt 0214 Ö	Alt 0246 ö
Alt 27 ←	<b>Equality</b>	Alt 183 ⊥	Alt 207 ▫	Alt 0155 ›	Alt 0218 Ù	Alt 0249 ú
<b>Bullets</b>	Alt 240 ≡	Alt 184 ⊥	Alt 208 ▬	Alt 0145 ´	Alt 0219 Û	Alt 0250 û
Alt 3 ♥	Alt 61 =	Alt 185 ⊥	Alt 209 ▭	Alt 0146 ´	Alt 0220 Ü	Alt 0251 ü
Alt 4 ♦	Alt 247 ≈	Alt 186	Alt 210 ▮	Alt 0147 " " " " " "	Alt 0217 Û	Alt 0252 ù
Alt 5 ♣	<b>Inequality</b>	Alt 187 ⊥	Alt 211 ▯	Alt 0148 " " " " " "	Alt 0221 Ý	Alt 0253 ý
Alt 6 ♠	Alt 60 <	Alt 188 ⊥	Alt 212 ▰	Alt 174 «	Alt 0159 Ÿ	Alt 0255 ÿ
Alt 7 •	Alt 62 >	Alt 189 ⊥	Alt 213 ▱	Alt 175 »	Alt 0142 Ž	Alt 0158 ž
Alt 8 ▣	Alt 242 ≥	Alt 190 ⊥	Alt 214 ▲	Alt 0130 ´	<b>"Extra" Letters</b>	
Alt 9 ○	Alt 243 ≤	Alt 191 ⊥	Alt 215 △	Alt 0132 „	<b>Uppercase</b>	<b>Lowercase</b>
Alt 10 ☐	<b>Powers</b>	Alt 192 ⊥	Alt 216 ▴	<b>Abbrevs.</b>	Alt 0229 à	Alt 0197 Å
Alt 11 ♂	Alt 251 √	Alt 193 ⊥	Alt 217 ▵	Alt 39 ´	Alt 0140 Œ	Alt 0156 œ
Alt 12 ♀	Alt 252 °	Alt 194 ⊥	Alt 218 ▹	Alt 96 ´	Alt 0254 þ	Alt 0222 þ
Alt 13 ♪	Alt 0185 ¹	Alt 195 ⊥	Alt 219 ▸	Alt 38 &	Alt 0216 Ø	Alt 0248 ø
Alt 14 ♫	Alt 0178 º	Alt 196 ⊥	Alt 220 ▹	Alt 64 @	Alt 0198 Æ	Alt 0230 æ
Alt 16 ►	Alt 0179 ¸	Alt 197 ⊥	Alt 221 ▹		Alt 164 ñ	Alt 165 Ñ
Alt 17 ◄	<b>Angles/Trig</b>	Alt 198 ⊥	Alt 222 ▹		Alt 0223 ß	
Alt 254 ▣	Alt 227 π	Alt 199 ⊥	Alt 223 ▹		Alt 0208 Đ	Alt 0240 đ
Alt 30 ▲	Alt 248 °				<b>Coding</b>	
Alt 31 ▼	<b>General Maths</b>	<b>General Punctuation</b>			Alt 0166 ¡	Alt 92 \
Alt 23 ↑	Alt 35 #	Alt 58 :	Alt 0133 ...	Alt 45 -	Alt 40 (	Alt 35 #
Alt 24 ↑	Alt 236 ∞	Alt 59 :	Alt 95 =	Alt 0151 —	Alt 41 )	Alt 40 (
Alt 25 ↓	Alt 230 μ	Alt 44 ,	Alt 0175 =	Alt 22 —	Alt 94 ^	Alt 41 )
Alt 26 →	Alt 228 Σ	Alt 46 .	Alt 124	Alt 42 *	Alt 60 <	Alt 64 @
Alt 27 ←	Alt 239 ∩	Alt 32 ~	Alt 126 ~	Alt 47 /	Alt 62 >	Alt 91 [
Alt 0129 ☐	<b>Cardinals</b>	Alt 255 ¨	Alt 0168 ¨	Alt 92 \	Alt 61 =	Alt 93 ]
Alt 15 ☆	Alt 166 ª	Alt 65 - 90 A to Z	Alt 249 -		Alt 42 *	Alt 123 {
Alt 127 △	Alt 167 °	Alt 97 - 122 a to z	Alt 250 -		Alt 47 /	Alt 125 }
Alt 18 ↑	<b>Interpunct</b>	Alt 244 [	Alt 170 ~			
Alt 29 ↔	Alt 0183 ·	Alt 245 ]				