פרויקט גמר באסמבלי – ספר פרויקט

מגיש: דניאל ריימן

מורה: שרה יחיאל

שנה: 2024

בית ספר: תיכון הראשונים

נושא: אלגוריתמים

תוכן עניינים

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:

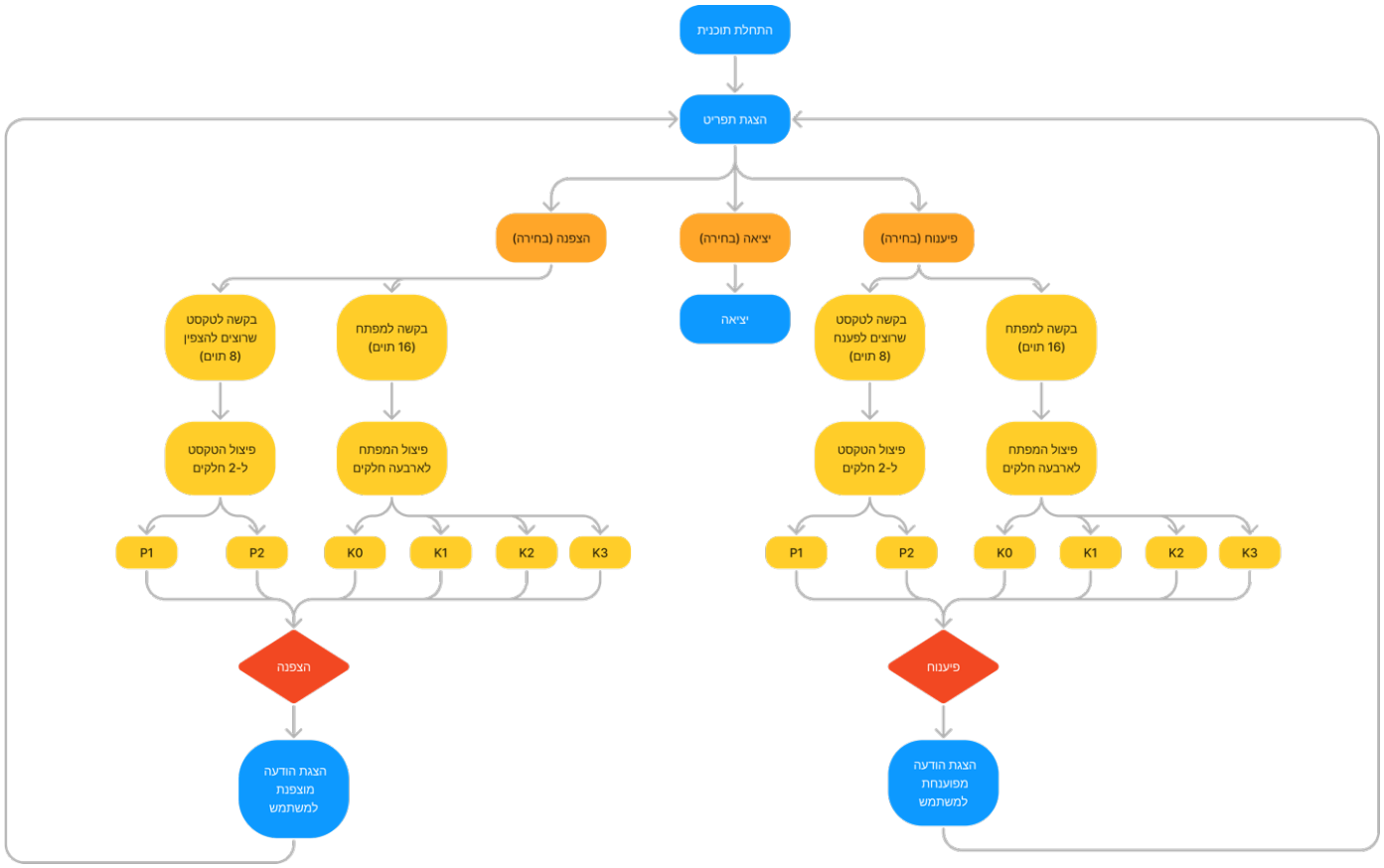
    טקסט: 64 bits

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

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

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 √, יש ללחוץ על Alt ובאותו הזמן להקיש במקש המספרי של המקלדת את 251, כלומר:

  Alt + 251 = √

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

Alt 1	☺
Alt 2	☻
Alt 3	♥
Alt 11	♂
Alt 12	♀
Alt 13	♪
Alt 14	♫

IP

Alt 0169	©
Alt 169	®
Alt 0153	™

Filled Arrows

Alt 16	►
Alt 17	◄
Alt 254	■
Alt 30	▲
Alt 31	▼

Line Arrows

Alt 23	↨
Alt 24	↑
Alt 25	↓
Alt 26	→
Alt 27	←

Bullets

Alt 3	♥
Alt 4	♦
Alt 5	♣
Alt 6	♠
Alt 7	•
Alt 8	◘
Alt 9	○
Alt 10	◙
Alt 11	♂
Alt 12	♀
Alt 13	♪
Alt 14	♫
Alt 16	►
Alt 17	◄
Alt 254	■
Alt 30	▲
Alt 31	▼
Alt 23	↨
Alt 24	↑
Alt 25	↓
Alt 26	→
Alt 27	←
Alt 0129	Box
Alt 15	☼
127	⌂
Alt 18	↕
Alt 29	↔

Numbers

Alt 48 - 57	0 - 9

Basic Operators

Alt 43	+
Alt 45	-
Alt 0215	×
Alt 0247	÷

Pers

Alt 37	%
Alt 0137	‰

Bracketing

Alt Code	Symbol
Alt 40	(
Alt 41	)

Plus or Minus

Alt 241	±

Fractions

Alt 47	/
Alt 0188	¼
Alt 0189	½
Alt 0190	¾
Alt 46	.

Equality

Alt 240	≡
Alt 61	=
Alt 247	≈

Inequality

Alt 60	<
Alt 62	>
Alt 242	≥
Alt 243	≤

Powers

Alt 251	√
Alt 252	ⁿ
Alt 0185	¹
Alt 0178	²
Alt 0179	³

Angles/Trig

Alt 227	π
Alt 248	°

General Maths

Alt 35	#
Alt 236	∞
Alt 230	µ
Alt 228	Σ
Alt 239	∩

Cardinals

Alt 166	ª
Alt 167	º

Interpunct

Alt 0183	·

Greek

Alt 224	α
Alt 225	ß
Alt 226	Γ
Alt 235	δ
Alt 238	ε
Alt 233	Θ
Alt 227	π
Alt 230	µ
Alt 228	Σ
Alt 229	σ
Alt 231	τ
Alt 232	Φ
Alt 237	φ
Alt 234	Ω

Currency

Alt 0164	¤
Alt 156	£
Alt 0128	€
Alt 36	$
Alt 155	¢
Alt 157	¥
Alt 158	Pts
Alt 159	ƒ

Accents

Alt 0180	´
Alt 0184	¸

Drawing

Alt 176	░	Alt 200	╚
Alt 177	▒	Alt 201	╔
Alt 178	▓	Alt 202	╩
Alt 179	│	Alt 203	╦
Alt 180	┤	Alt 204	╠
Alt 181	╡	Alt 205	═
Alt 182	╢	Alt 206	╬
Alt 183	╖	Alt 207	╧
Alt 184	╕	Alt 208	╨
Alt 185	╣	Alt 209	╤
Alt 186	║	Alt 210	╥
Alt 187	╗	Alt 211	╙
Alt 188	╝	Alt 212	╘
Alt 189	╜	Alt 213	╒
Alt 190	╛	Alt 214	╓
Alt 191	┐	Alt 215	╫
Alt 192	└	Alt 216	╪
Alt 193	┴	Alt 217	┘
Alt 194	┬	Alt 218	┌
Alt 195	├	Alt 219	█
Alt 196	─	Alt 220	▄
Alt 197	┼	Alt 221	▌
Alt 198	╞	Alt 222	▐
Alt 199	╟	Alt 223	▀

?s and !s

Alt 33	!
Alt 19	‼
Alt 173	¡
Alt 63	?
Alt 168	¿

Brackets

Alt 40	(
Alt 41	)
Alt 91	[
Alt 93	]
Alt 123	{
Alt 125	}

Editing

Alt 28	∟
Alt 21	§
Alt 20	¶
Alt 0134	†
Alt 0135	‡

Quotes

Alt 34	"
Alt 0139	‹
Alt 0155	›
Alt 0145	‘
Alt 0146	’
Alt 0147	“
Alt 0148	”
Alt 174	«
Alt 175	»
Alt 0130	‚
Alt 0132	„

Abbrevs.

Alt 39	'
Alt 96	`
Alt 38	&
Alt 64	@

Letters with Accents

Uppercase		Lowercase	
Alt 0192	À	Alt 0224	à
Alt 0193	Á	Alt 0225	á
Alt 0194	Â	Alt 0226	â
Alt 0195	Ã	Alt 0227	ã
Alt 0196	Ä	Alt 0228	ä
Alt 0199	Ç	Alt 0231	ç
Alt 0200	È	Alt 0232	è
Alt 0201	É	Alt 0233	é
Alt 0202	Ê	Alt 0234	ê
Alt 0203	Ë	Alt 0235	ë
Alt 0204	Ì	Alt 0236	ì
Alt 0205	Í	Alt 0237	í
Alt 0206	Î	Alt 0238	î
Alt 0207	Ï	Alt 0239	ï
Alt 165	Ñ	Alt 164	ñ
Alt 0210	Ò	Alt 0242	ò
Alt 0211	Ó	Alt 0243	ó
Alt 0212	Ô	Alt 0244	ô
Alt 0213	Õ	Alt 0245	õ
Alt 0214	Ö	Alt 0246	ö
Alt 0138	Š	Alt 0154	š
Alt 0218	Ú	Alt 0249	ú
Alt 0219	Û	Alt 0250	û
Alt 0220	Ü	Alt 0251	ü
Alt 0217	Ù	Alt 0252	ù
Alt 0221	Ý	Alt 0253	ý
Alt 0159	Ÿ	Alt 0255	ÿ
Alt 0142	Ž	Alt 0158	ž

"Extra" Letters

Uppercase		Lowercase	
Alt 0229	å	Alt 0197	Å
Alt 0140	Œ	Alt 0156	œ
Alt 0254	þ	Alt 0222	Þ
Alt 0216	Ø	Alt 0248	ø
Alt 0198	Æ	Alt 0230	æ
Alt 164	ñ	Alt 165	Ñ
Alt 0223	ß		
Alt 0208	Ð	Alt 0240	ð

General Punctuation

Alt 58	:	Alt 0133	…	Alt 45	-
Alt 59	;	Alt 95	_	Alt 0151	—
Alt 44	,	Alt 0175	¯	Alt 22	▬
Alt 46	.	Alt 124	|	Alt 42	*
Alt 32		Alt 126	~	Alt 47	/
Alt 255		Alt 0168	¨	Alt 92	\

Miscellaneous

Alt 65 - 90	A to Z	Alt 249	·
Alt 97 - 122	a to z	Alt 250	·
Alt 244	⌠	Alt 170	¬
Alt 245	⌡		

Coding

Alt 0166	¦	Alt 92	\
Alt 40	(	Alt 35	#
Alt 41	)	Alt 40	(
Alt 94	^	Alt 41	)
Alt 60	<	Alt 64	@
Alt 62	>	Alt 91	[
Alt 61	=	Alt 93	]
Alt 42	*	Alt 123	{
Alt 47	/	Alt 125	}