תיק פרוייקט aes 128b encryption

תכנית: תוכנת פענוח והצפנה של AES

מגיש: עילאי סמואלוב

כיתה: י9

בית ספר: ליידי דייויס תל אביב

1. מטרת הפרוייקט

מטרת הפרוייקט הייתה לכתוב תוכנה בשפת אסמבלי שתהיה מסוגלת להצפין BLOCK של 16 תווים וגם לפענח BLOCK

של 16 תווים תוך שימוש באלגוריתם ההצפנה AES 128b.

בהמשך הכתיבה גם הוספתי אופציה של הצפנה של מסמך שלם.

בסיום הפרוייקט רכשתי יכולות כמו:

ידע בקריפטוגרפיית AES

קליטת ערכים משהמשתמש

המרה של ערכים

הגדרה של מטריצה(מערך)

שימוש בפעולות לוגיות ומתמטיות כמו XOR ו AND

מתמטיקה תחת שדה אלגברי בשם GALIOS FIELD של 2^8

2.תיאור התכנית

התכנית מצפינה ערכים באמצעות אלגורית ההצפנה AES.

זהו סוג של אלגוריתם הצפנה יעיל ואפקטיבי שמצפין ערכים ביעילות גבוהה.

AES נוצר על ידי שני מתמטיקאים בשם ריימן ודאמן.

ההצפנה קולטת ערכים בגודל 128B ומעבירה אותם המון טרנספורמציות שנקבעות על ידי מפתח ההצפנה.

כל ההגיון מאחורי הצפנה הוא שניתן להחזיר את הטקסט המוצפן לקדמותו תוך שימוש במפתח ההצפנה ולכן בכתיבת האלגוריתם צריך לשים לב לסבך את הטקסט כמה שיותר מבלי לאבד ערכים ומבלי לצרוך המון משאבים מהמחשב. AES היה בין הראשונים לעשות זאת והוא נבחר על ידי הNSA להצפנה של TOP SECRET INFORMATION.

לפני כתיבת התכנית למדתי לפרטי פרטים את אלגוריתם ההצפנה.

האלגוריתם מעט מסובך והוא לקח לי קרוב לחודשיים ללמוד בוודאות את הכל(הצפנה ופענוח).

ורק לאחר שבאמצעות מחשבון דף ונייר הצלחתי להצפין בלוק סיבוב אחד של AES ידעתי שאני יודע טוב את האלגוריתם ואני מוכן להתחיל לכתוב.

של הכתיבה של הקוד לקח לי קרוב לשבועיים.

3.ביבליוגרפיה

במהלך התכנית, בנוסף לידע באסמבלי הייתי צריך ללמוד לפרטי פרטים כיצד אלגוריתם ההצפנה עובד והיו לי המון קשיים בהתחלה מכייוון שזה המון חומר וכל מקור אומר דבר אחר.

אך לאחר חקירה מצאתי את המקורות האלה שמאוד עזרו לי להצליח בפרוייקט:

באתר הבא העזרתי בשביל האינטראפטים השונים שאיתם עבדתי:

http://spike.scu.edu.au/~barry/interrupts.html

באתר הזה נעזרתי בשביל הDEBUGGING לתכנית.

https://www.kavaliro.com/wp--content/uploads/2014/03/AES.pdf

בסרטון הבא נעזרתי בשביל כתיבת של ה MIX COLUMNS

https://www.youtube.com/watch?v=JWJXCWt-fJo

באתר הבא נעזרתי בשביל הבנת אלגוריתם ההצפנה לפרטי פרטים:

https://arxiv.org/ftp/arxiv/papers/1209/1209.3061.pdf

באתר הבא נעזרתי בשביל הבנת השדה האלגברי של גאליוס

(https://en.wikipedia.org/wiki/GF(2

באתר הבא נעזרתי בשביל טבלאות המכפלה של ריינדול:

https://en.wikipedia.org/wiki/Rijndael_MixColumns

4.תיאור האלגוריתם

אלגוריתם ההצפנה קולט מהמשתמש מפתח ובלוק של 16 תווים להצפין.
המטריצה והמפתח יוכנסו אנכית לתוך מטריצה של 4על4.

לפני סדר האלגוריתם נגדיר את הטרנספורמציות הבסיסיות בקצרה:

1.ADDROUNDKEY זו הפעולה שאחראית על XOR בין ערכי ההודעה לערכי המפתח.

2.SUBBYTES זו הפעולה שאחראית על החלפת כל תו ותו לפי ערכי הNUBBLES שלו בערך אחר שנמצא במטריצה ייעודית בשמSBOX.

הניבל הגבוהה הוא השורה והניבל הנמוך הוא העמודה.

3.SHIFT ROWS פעולה הפונה למטריצה והחל מהשורה השנייה במטריצה מתחילה לעשות ROTATION שמאלה:

לשורה השנייה פעם אחת.

לשורה השלישית פעמיים.

לשורה הרביעית שלוש פעמים.

MIX_COLUMNS.4

הפעולה המורכבת ביותר בכל אלגוריתם ההצפנה ומהווה את החלק החשוב ביותר בה.

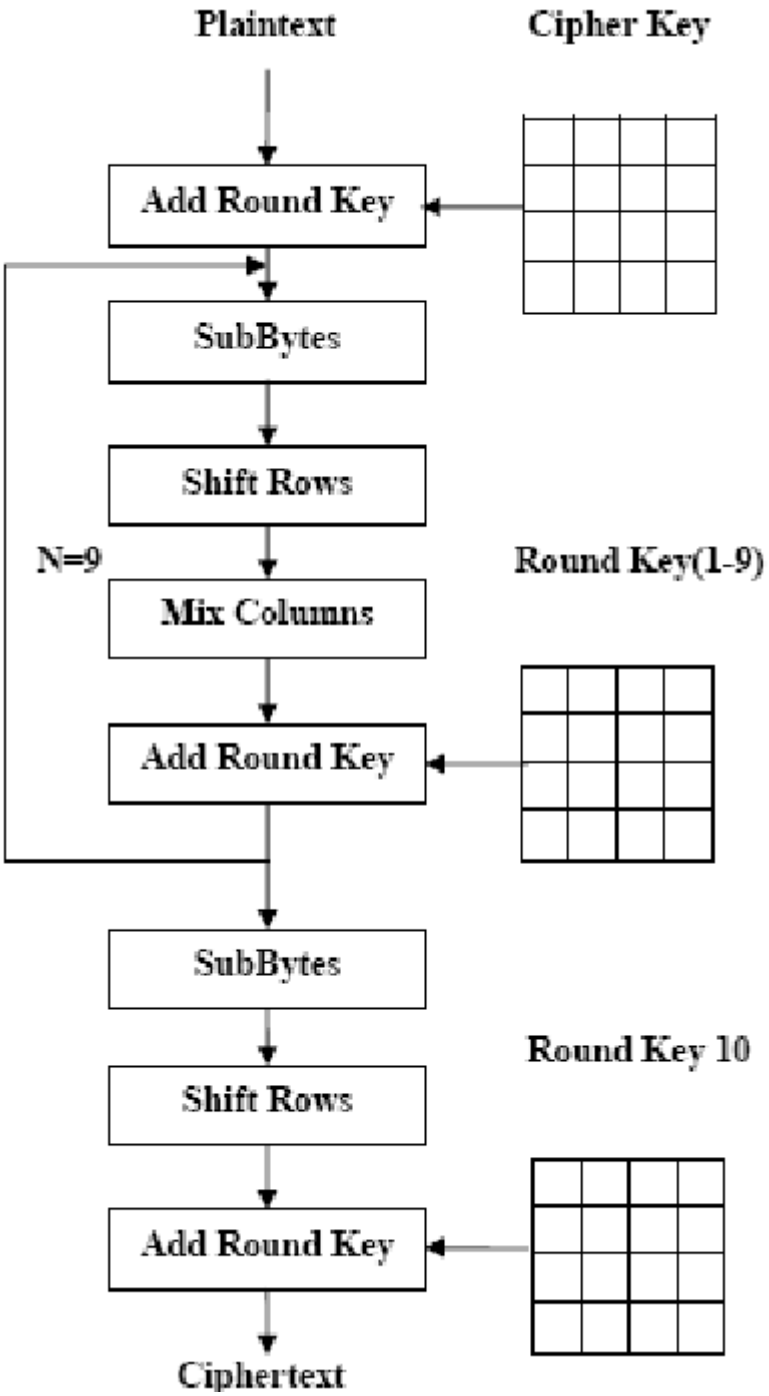
הפעולה מסתכלת על כל ערך במטריצת הבלוק ובודקת באזיה שורה הוא נמצא. לאחר מכן נלך לאותה השורה במטריצה ייעודית בשם MULTIPLYCATION ונכפול את העמודה של הערך במטריצת הבלוק בשטרה של מטריצת המכפלות.

לאחר מכן ניקח את השורה ונבצע XOR בין כל ארבעת ערכיה. הערך שמתקבל יחליף את הערך הראשוני עליו הסתכלנו במטריצת הבית.

5.תהליך יצירת המפתחות.

ההצפנה עוברת 10 סיבובים בהם בכל סיבוב מבצעים XOR בין כל ערך במפתח לכל ערך בבלוק. בשביל לשמור על סיבוך ולא להשתמש כל פעם באותו המפתח יש פעולה שמייצרת במהירות ובקלות מפתחות חדשים בכל סיבוב.

לאחר בגדרת הפעולות ניתן לראות בתרשים את סידרם כך שכל הפעולות בתבצעות על מטריצת הבלוק 10 פעמים:


Plaintext
Cipher Key
Add Round Key
SubBytes
Shift Rows
N=9
Round Key(1-9)
Mix Columns
Add Round Key
SubBytes
Round Key 10
Shift Rows
Add Round Key
Ciphertext

5.הפרוצדורות בפרוייקט:

proc Clear_ALL_Register

פעולה המנקה את כל הרגיסטרים

proc multiply2

פעולה שכופלת ב2 בשדה גאליוס

proc multiply3

פעולה שכופלת ב3 בשדה גאליוס

proc multiply1

פעולה שכופלת 1 בשדה גאליוס

proc inserttotemp1

פעולה שמכניסה עמודה למערך זמני

proc inserttotemp

פעולה שמכניסה עמודה למערך זמנית

proc inserttotemp3

פעולה שמכניסה מערך לשורה זמנית

proc multiply_tempcol_once

פעולה המבצעת מכפלה של שורה פעם אחת

proc multiplyall

פעולה שמזמנת את מכפלה של פעם אחת כלפי כל המטריצה

proc xortempcol

פעולה שעוסה אקסור על כל העמודה הזמנית

proc mixcol1

פעולה שמבצעת ערבוב שורות לשורה ראשונה

proc mixcol4

פעולה שמבצעת ערבוב שורות לשורה רביעית

proc CopyAfterMix_ColumnsTotArranged_Message

פעולה המעתיקה את מטריצת ערבוב השורות למטריצת הבלוק

proc Mix_Columns

פעולה שמזמנת את כל הפעולות שנכתבו למעלה על מנת לבצע את שלב ערבוב השורות

proc Keys_Expansion

פעולה שמבצעת את שלב יצירת המפתחות

proc Arrange_Array_Key

פעולה שמסדרת את המפתח במטריתה אנכית

proc Byte_Substitution

פעולה שמבצעת את שלב החלפת הבתים

proc Arrange_Array

פעולה שמסדרת את המערך אנכית במטריצה

proc Shift_Rows

פעולה שמבצעת את שלב חיסור השורות הסיבובי כלפי המטריצה

proc Add_Round_Key

פעולה שעטשה אקסור לכל ערך בבלוק עם כל ערך במפתח בהתאמה

<u>החל מכאן זהו חלק הפענוח</u>

proc input_key

פעולה שקולטת מהמשתש מפתח

proc shl_every_round_for_rcon

פעולה שעושה למטריצת הערך הסיבוב רוטציה בכל סיבוב של הצפנה

proc Print_Out_CipherText

פעולה המדפיסה את הערך הבופי של ההצפנה

proc input_cipherkey

פעולה הקולטת מפתח

proc input_ciphertext

פעולה הקולטת טקסט מוצפן

proc Arrange_Array_cipherkey

פעולה המארגנת אנכית את המפתח

proc Arrange_Array_ciphertext

פעולה המארגנת אנכית את הטקסט

proc Inverse_Byte_Substitution

הפעולה ההופכית להחלפת הבתים

proc Inverse_Shift_Rows

הפעולה ההופכית לחיסור השורות

proc mul9

פעולת כפל ב9 תחת שדה גאליוס

proc mul11

פעולה הכופלת ב11 תחת שדה גאליוס

proc mul13

פעולה הכופלת ב13 תחת שדה גאליוס

proc mul14

פעולה הכופלת ב14 תחת שדה גאליוס

proc Multiplytempcol_once_inverse

פעולה המבצעת כפל של שורה פעם אחת

proc multiplyall_inverse

פעולה המזמנת את הפעולה שלמעלה כלפיי כל המטריצה

proc xortempcol_inverse

פעולה העושה אקסור לעמודה הזמנית

proc inserttotempinverse1

פעולה המכניסה שורה אחת לשמנית

proc inserttotempinverse2

פעולה המכניסה שורה שנייה לזמנית

proc inserttotempinverse3

פעולה שמכניסה 3 לזמנית

proc inserttotempinverse

פעולה המכניסה שורה 0 לזמנית

proc mixcol1_inverse

פעולת ערבוב שורות לשורה 1

proc mixcol4_inverse

פעולת ערבוב שורוצ לשורה 4

proc CopyAfterMix_ColumnsTotArranged_Message_inverse

פעולה המעתיקה לבלוק הראשי את התוצאות מערבוב השורות

proc Inverse_Mix_Columns

פעולת ראשית לשלב ערבו השורות המזמנת את שאר הפעולות

proc Inverse_Add_RoundKey

פעולה המוסיפה את המפתח לבלוק

proc Inverse_Keys_Expansion

פעולה הופכית ליצירת המפתחות

proc All_Round_Inversed_Key

פעולה המעתיקה בסדר הפוך את כל המפתחות

proc Update_Cipherkey

פעולה הדואגת לעדכן מפתח בכל סיבוב

proc copkey

פעולה המעציקה מפתח

proc lastrndkey

פעולה הדואגת להוסיף את המפתח האחרון לבלוק

proc ciphertext_to_final

פעולה המכניסה את הטקסט שפועמח למטריצה סופית

proc File_Encryption_Guide

פעולה המציגה למשתמש הדרכה על הצפנת קובץ

proc input_file_name

פעולה הקולטת שם קובץ

proc Read_16b

פעולה הקוראת מהמסמך 16 בתים

proc Copy_To

פעולה המעתיק הת 16 הבתים

proc Encrypt_16b

פעולה שמצפינה את 16 הבתים שנקלטו

proc Write_16b

פעולה הכותבת למסמך החדש את מה שהוצפן

proc calc_file_size

פעולה המחשבת כמה סיבובי הצפנה יש לעשות לפי גודל המסמך

proc Keep_Key_Safe_copy

פעולה המונעת דריסה של המפתח המקורי

proc Create_new_file

פעולה היוצרת קובץ חדש

proc ReCreate_Original_Key

פעולה שיוצקת מפתח מקורי חדש בשביל המשפט הבא במסמך

proc Encrypt_128_bits_Block_In_Plain_Text

פעולה המצפינה בלוק

proc Decrypt_128_bits_Block_in_Plain_Text

פעולה המפענחת בלוק

proc Encrypt_File_using_aes_128b;//////

פעולה המצפינה מסמך שלם

proc menu

פעולת תפריט שמנהלת את כל הפרוייקט ונותנת למשתמש אופציית בחירה לאיזה אפשרות הוא ירצה לעשות. למעשה אין תוכנית ראשית.

השורה היחידה בתוכנית הראשית היא זימון פעולת התפריט שתנהל את הכל בעצמה.