שם המגיש: עומר גרייף

ת"ז : 2082000154

תאריך הגשה: 31/5/23

<u>שאלה 2 – AES,Modes of operations</u>

1. איכותו של צופן AES מתבסס על כך שמבצעים פעולות איטרטיבות על הבלוק כך שכל פעולה תוסיף רובד של קושי בתרגום הצופן. הסטודנט מעוניין להוריד את פעולת MIX_COLUMNS שתפקידה לבצע פעולה על כל איבר בבלוק כך שתיווצר תלות בערך החדש שלו לבין כל האיברים שנמצאים איתו באותה עמודה. נזכיר כי שאר השלבים דואגים ליצור ערבוב של שאר המאפיינים כמו בתים בודדים,שורות וbyte-wise XOR . אם זאת ללא שלב הMIX_COLUMNS כל שינוי של בית בבלוק ישפיע רק על בית אחד בבלוק המוצפן. בנוסף לכך גם הפעולה של הסטודנט המעוניין לבצע rotate-clockwise גוררת הזזה של האיברים בלבד ללא יצירת תלות בין ערכי האברים ועל כן גורמת לכך ששינוי של בית בבלוק המקורי תשפיע אך ורק על בלוק אחד ועל כן האלגוריתם שהסטודנט מציע צפוי להיות יותר "קל ומהיר" לפריצה מאשר האלגו המקורי.
לצורך התקפת chosen-plaintex נבנה טבלה שתתבסס על המידע הבא:
בלוק בגודל 128 ביט ו16 תאים -> כל תא מכיל 8 ביט => 2^8 אופציות לתא => ממספר האופציות לתא + השפעה של כל בית בבלוק המקורי בבלוק בודד בבלוק המוצפן => מספיקים 2^8 זוגות של P,C על מנת לפענח את הקוד (נדרוש בלוקים כך שבסה"כ עבור כל תא בנפרד נעבור על כל האופציות האפשריות).
סיבוכיות מקום -> כל זוג *P,C* כולל 2 בלוקים כלומר *2*128bit* .אנו צריכים לשמור 2^8 זוגות לכן נקבל סה"כ $2^{16}bit$
סיבוכיות זמן-> סיבוכיות הזמן לפענוח והצפנה היא בהתאם לבניית הטבלאות שהן $2^8 * 2 = 2^9$
2. ההצעה לשיפור אינה טובה ותפגע בחסינות האלגוריתם. זאת מכיוון שbyte substitution היא הפעולה היחידה הלא לינארית באלגוריתם. ברגע שנסיר אותה ונחליף אותה בפועלה לינארית כלשהי נקבל שכל פעולות האלגוריתם לינאריות כלומר האלגוריתם הוא לינארי. לכן ניתן בקלות יחסית לפענח את הצופן על ידי זוג בודד של C,P כיוון שנקבל C=F(P)*G(K).
כלומר נפיק F(P) נחלץ G(K) ונוכל לפענח ולהצפין בקלות יחסית לעומת קיום פעולה לא לינארית שלא מאפשרת פירוק זה.
3. הצופן הנתון חזק לפחות כמו הצופן המקורי. באלגוריתם זה נבחין כי ראשית לא גרענו מאף שלב באלגוריתם -> השארנו את האי לינאריות, את התלות של כל איבר בעמודה שבה הוא נמצא בשלב מסוים באלגוריתם. כלומר אם נסתכל על תרשים של השפעת האלגוריתם עבור איבר בודד בבלוק נקבל שמספר האיברים שתלויים בו/הוא בהם הוא בסדר גודל זהה לאלגוריתם החדש ויותר, ועל כן הצופן קשה לפחות כמו האלגוריתם שלנו.
4. א. הבעיה בשימוש באופן תפעול זה היא שהצפנת הבלוקים בנפרד ללא תלות לבלוקים האחרים תגרום לכך שבלוקים זהים יעברו את אותה טרנספורמציה. מכיוון שקובץ וידאו מכיל המון מידע ויזאולי טרנספורמציה שלו אמנם תפגע באיכות התמונה/צבעים אך עדיין יהיה ניתן להבין מה מתרחש בוידאו המקובל. זאת מכיוון שכל בלוק זהה עובר טרנספורמציה זהה כפי שראינו בתרגול בדוגמה עם הפינגווין. ועל כן הצפנה זו פחות מתאימה להעברת וידאו.

ב. כדי לפתור בעיה זו ניתן להשתמש באופן תפעול *CBC* שיוצר תלות בין הבלוקים (משרשר את הצפנת הבלוק הקודם לחישוב הבלוק הבא) ועל כן לאחר הצפנה שכזו נקבל תמונה לא ברורה שלא תהיה קלה לפענוח כיוון שבלוקים זהים כבר לא יוצפנו לבלוקים זהים.

5. א. *ECB*: הודעה 1 -> *BLOCK_A BLOCK_A*
הודעה 2 -> *BLOCK_A BLOCK_B*
(כאשר *BLOCK_A* שונה מ*BLOCK_B* ושניהם באורך בלוק של האלגו). כעת ייתכנו 2 מקרים לאחר הצפנה של אחת ההודעות : אם קיבלנו 2 בולקים שחוזרים על עצמם סימן שהצפנו את הודעה מספר 1, זאת מכיוון שבלוקים זהים מתורגמים לאותו בלוק לאחר הצפנה. לא ייתכן שנקבל שבלוק אחר יתורגם לאותו בלוק מטעמי חד חד ערכיות. לכן, אם נקבל 2 בלוקים שונים אזי נדע שקיבלנו את הודעה 2.
ב. *Interleaved-CBC*: הודעה 1 -> *BLOCK_A BLOCK_A*
הודעה 2 -> *BLOCK_A (BLOCK_B XOR 34)*
(כאשר *BLOCK_A* שונה מ0 ובתנאים כמוסבר בסעיף א.)

על פי הגדרת האלגוריתם ההצפנה שתתבצע תהא:

עבור *C1*: $C1 = E(M1\ XOR\ IV0)$

עבור *C2*: $C2 = E(M2\ XOR\ IV1) = E(M2\ XOR\ (IV0\ XOR\ 34))$

נבחין כי עבור *M1* ו *M2* זהים נקבל פלטים שונים לאחר ההצפנה לאור ביצוע *XOR*.

אם זאת עבור הדוגמה כפי שהגדרנו בהודעה 2 נקבל ל*C2* :

$$C2 = E(M2\ XOR\ (IV0\ XOR\ 34)) = E(M1\ XOR\ 34\ XOR\ (IV0\ XOR\ 34)) = E(M1\ XOR\ IV0))$$

נבחין כי עבור *M1* ו*M2* כפי שהוגדרו בהודעה 2 נקבל הצפנה זהה לשתי הבלוקים.

ועל כן קיבלנו יכולת להבחין באיזו הודעה מדובר לאחר הצפנה.

6. מכיוון שבכל שלב עומר יודע את ה*IV* הבא ולפחות את הקודם כיוון שהם משודרים וגלויים לכולם. הוא יכול לתפוס את ההודעה ברגע *prev* כולשהו כאשר ברשתו גם מפתח *next*. כעת הוא יכול לשלוח כן או לא (נבחר בה"כ כן) עם *XOR* מפתח *prev* ו*XOR* מפתח *next* ולהשוות לערך שהוא האזין לו בשיחה של יורי עם רועי. אם יתקבל ערך זהה נדע שהועבר כן אחרת לא. כעת אסביר את הנכונות, מכיוון שאם נשרשר כן (בה"כ) עם *XOR* מפתח *prev* ו*XOR* מפתח *next* בזמן *next* נבטל את תלות ה*XOR* הנ"ל ונשאר רק עם כן*XOR*מפתח*next* שלאחר הצפנה יהיה זהה לפעולת ההצפנה שעברה ההודעה בין יורי לרועי וכך נוכל להשוות את התוצאה. אם התוצאה זהה נדע שעבר כן על בסיס הנחת הבה"כ ואחרת שלא.