

המחלקה למדעי המחשב

סמינר בקריפטוגרפיה

20374

הצפנות סימטריות DES ו-AES וחסינותם

שם הסטודנט: רז עטר

ת"ז סטודנט: 201528775

מנחה: ד"ר מיקולינסקי ולדימיר

מרכזת הוראה: ד"ר הרמן מעינה

סמסטר: 2015 ב'

תאריך הגשה : 18/07/2015

תוכן עניינים

1. מבוא .............................................................................................................. 3
2. סקירה ומונחים.................................................................................................4
3. קריפטאנליזה....................................................................................................6
   1. הקדמה.......................................................................................................6
   2. סוגי התקפות...............................................................................................6
   3. סוגי בטיחות................................................................................................6
4. Data Encryption Standard...............................................................................8
   1. רקע היסטורי...............................................................................................8
   2. תיאור DES..................................................................................................8
   3. בטיחות וחסינות DES...................................................................................11
   4. DES2 ו-3DES ובטיחותם...............................................................................20
5. Advanced Encryption Standard......................................................................22
   1. רקע היסטורי...............................................................................................22
   2. תיאור AES..................................................................................................22
   3. בטיחות וחסינות AES...................................................................................25
6. סיכום ומסקנות.................................................................................................28
7. רשימה ביבליוגרפית...........................................................................................29
8. נספח - מושגים כלליים.......................................................................................30
9. **מבוא**

בעולם ההצפנה ישנם שני חברים טובים מאוד, אליס (Alice) ובוב (Bob). אליס ובוב הם שני גורמים שיש להם צורך לתקשר מעל גבי ערוץ תקשורת בלתי אמין, ומבקשים להנות מסודיות. כיצד נוכל למנוע מגורם עוין שעלול לצותת לשיחתם לצפות במידע הרגיש שעובר על גבי ערוץ התקשורת?   
פיתרון: הצפנת מידע- אליס ובוב משתמשים **בצופן** (cryptosystem) קיימים שני סוגים של הצפנות: הצפנה סימטרית והצפנה א-סימטרית. בעבודה זו נתמקד בפיתרון הצפנה הסימטרית (ובפרט בהצפנות DES ו-AES). תחילה נסקור מונחים בסיסיים בנושא זה ונתאר את ענף הקריפטאנליזה. לאחר מכן, נתמקד באלגוריתמי הצפנה DES ו-AES : נתאר את הצפנות אלו, נבדוק אלו תקיפות קיימות על אלגוריתמי הצפנה אלו ונסיק האם הצפנות אלו חסינות.

1. **סקירה ומושגים**להלן סקירה ומושגים כפי שמתואר ב-[1].
2. **צופן:**

חמישייה (P,C,K,E,D) כאשר:

* P - קבוצה סופית המהווה את אוסף יחידות הטקסט הגלוי.
* C - קבוצה סופית המהווה את אוסף יחידות הטקסט המוצפן.
* K - מרחב המפתחות, קבוצה סופית של מפתחות אפשריים להצפנה.
* E - פונקציית הצפנה על טקסט גלוי  ומפתח , .
* D- פונקציית פענוח על טקסט מוצפן  ומפתח , .
* פונקציית ההצפנה חייבת להיות חד חד ערכית, ולקיים שלכל ,  מתקיים .

1. **הצפנה סימטרית:**  
   אלגוריתם הצפנה המשתמש במפתח אחד גם להצפנת המידע וגם לפענוחו.  
   הצפנה סימטרית היא הוותיקה ביותר ושורשיה החלו עם ההצפנה הקלאסית לפני מאות שנים.  
   אליס ובוב מסכימים ביניהם מראש על שיטה מסוימת להצפנה ועל מפתח (key). נניח שאליס מעוניינת לשלוח לבוב הודעה מסוימת. היא מצפינה (encrypt) את ההודעה בשיטה שהיא ובוב בחרו תוך כדי שימוש במפתח שהם קבעו. לאחר ההצפנה, ההודעה שינתה את צורתה. להודעה המקורית אנו קוראים טקסט גלוי (plaintext), ולהודעה אחרי ההצפנה קוראים טקסט מוצפן (ciphertext). אליס שולחת את הטקסט המוצפן לבוב, ובוב מפענח (decrypt) אותו ומשחזר את הטקסט הגלוי.  
   ההנחה היא שגורם עוין שמאזין בערוץ התקשורת יתקשה מאוד לשחזר את הטקסט הגלוי מתוך הטקסט המוצפן, או אפילו חלק קטן מתוכו, ללא ידיעת המפתח.
2. **צופן בלוק (block cipher):**

צופן סימטרי איטרטיבי המצפין מחרוזת סיביות באורך קבוע הנקראת בלוק בטרנספורמציה קבועה, כלומר, מקבל בלוק של סיביות "טקסט גלוי" באורך קבוע n ומפתח הצפנה והפלט הוא בלוק טקסט מוצפן באורך קבוע n. באופן פורמאלי:   
E(K,P):\{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n  
פונקציית הפענוח היא הפונקציה ההופכית של E.

1. **צופן פייסטל:**

מבנה סימטרי המשמש לבניית צופני בלוקים הקרוי על שם ממציאו, המדען הגרמני-אמריקאי הורסט פייסטל. צופן פייסטל בנוי כך שהוא מחלק את הטקסט הגלוי לשני חלקים, ימין ושמאל. בכל איטרציה מופעלת פונקציית השלב על אחד הצדדים ובסופה מחברים את הצדדים באמצעות פעולת XOR. איטרציה הבאה מחליפים בין הצדדים כך שהפלט מהצד הימני הופך להיות הקלט לצד השמאלי ולהיפך.

1. **צופן SPN (Substitution-Permutation Networks)**:

רשתות החלפה-תמורה שבהן הפונקציה הפנימית מבוצעת על כל סיביות הקלט באופן אחיד, מקבלת בלוק מידע וחלק ממפתח ההצפנה ומבצעת מספר טרנספורמציות על סיביות הבלוק שנקראות מצב (state) במספר סבבים.

1. **קריפטאנליזה**
   1. **הקדמה**

בפרק זה נציג את נושא ניתוח צפנים - בטיחות, תקיפה ושבירת צופן. מטרת הפרק הינה לתת הקדמה לקראת ניתוח בטיחות וחסינות הצפנים DES ו-AES. כפי שמתואר ב-[1] ,  
**קריפטאנליזה** משמעותו ניתוח צפנים על מנת למצוא בהם נקודות תורפה שמאפשרות תקיפה או שבירה של צופן.   
**תקיפת צופן** היא אלגוריתם המאפשר למצוא את מפתח ההצפנה או טקסט גלוי (גם חלק ממנו) בסבירות לא זניחה ובזמן ריצה הקצר מזמן הריצה הנחוץ למעבר על כל מרחב המפתחות (Brute Force).  
**שבירת צופן** הינה תקיפה יעילה אשר זמן הריצה שלה הינו סביר ומהווה איום מעשי על הצופן.  
ההנחה הבסיסית בקריפטאנליזה הינה שיריב יודע מה אלגוריתם הצופן שנעשה בו שימוש וכל בטיחות הצופן תלויה בסודיות המפתח בלבד, מכיוון שיריב מתוחכם יצליח לגלות את אלגוריתם ההצפנה בקלות.

* 1. **סוגי התקפות**

כפי שמתואר ב- [1] ו-[2],

* התקפת טקסט מוצפן בלבד (ciphertext-only attack or known ciphertext attack):  
  סוג התקפה שבה מניחים שלתוקף יש גישה לטקסטים מוצפנים בלבד. לתוקף אין גישה לטקסטים גלויים ולכן הינה התקיפה הקשה ביותר לתוקף.
* התקפת טקסט גלוי ידוע (known plaintext attack):  
  סוג התקפה שבה לתוקף יש גישה לחלק מהטקסטים גלויים ולטקסטים המוצפנים בהתאמה, כלומר, קבוצת זוגות של טקסטים גלויים ומוצפנים בהתאמה.
* התקפת טקסט גלוי ניתן לבחירה (chosen plaintext attack):סוג התקפה שבה מניחים שהתוקף יכול לבחור אקראית טקסטים גלויים, להצפין אותם, ולקבל את הטקסטים המוצפנים התואמים. התקפה מסוג זה חשובה בעיקר בהקשר של הצפנה עם מפתח ציבורי, שבה מפתח ההצפנה הינו ציבורי והתוקף יכול להצפין כל טקסט שהוא בוחר.
* התקפת טקסט מוצפן ניתן לבחירה (chosen ciphertext attack):סוג התקפה שבה התוקף יכול לבחור טקסט מוצפן כרצונו, לפענח אותו (כאשר הוא לא יודע את המפתח) ולקבל את הטקסט הגלוי בהתאמה.
  1. **סוגי בטיחות**

כפי שמתואר ב-[1],

* בטיחות חישובית (computational security):   
  צופן הוא בעל בטיחות חישובית אם זמן הריצה של האלגוריתם הוא ארוך מאוד ולא מעשי.
* בטיחות יחסית (provable security):   
  צופן הוא בעל בטיחות יחסית ביחס לבעיה מתמטית כלשהי, אם הבעיה המתמטית נחשבת קשה, וניתן להוכיח שבעיית שבירת הצופן קשה לפחות כמו הבעיה המתמטית. ההוכחה נעשית באמצעות רדוקציה מהבעיה המתמטית לבעיית שבירת הצופן.
* בטיחות בלתי מותנית:   
  צופן הוא בעל בטיחות בלתי מותנית אם לא ניתן לשבור אותו גם באמצעות משאבי זמן ומקום אינסופיים.
* סודיות מושלמת:  
  מונח זה הוצג לראשונה ע"י קלוד שנון בשנת 1949. בהינתן צופן ננתח את בטיחות השימוש בו פעם אחת. לצופן יש סודיות מושלמת אם לכל  מתקיים: , כלומר, בהינתן טקסט מוצפן לא ניתן ללמוד כלום על הטקסט הגלוי. דוגמא לצופן בעל סודיות מושלמת הינו פנקס חד פעמי ( לא נדון בנושא זה בעבודה).

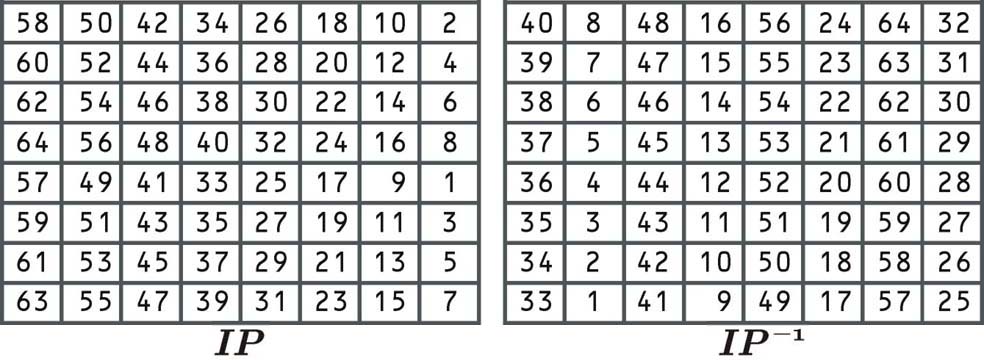
1. **Data Encryption Standard (בראשי תיבות DES)**
   1. **רקע היסטורי**

ע"פ [1] , Data Encryption Standard (בראשי תיבות DES) הינו תקן ופיתרון להצפנת נתונים שבפותח ע"י חברת IBM בשיתוף ה-NSA ופורסם לראשונה במאי 1975 ע"י המכון הלאומי לתקנים וטכנולוגיה (NIST).

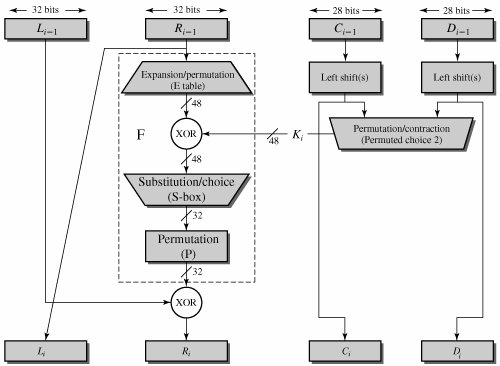
* 1. **תיאור DES**

כעת נתאר את DES ע"פ [1]:

* DES הינו צופן בלוקים סימטרי איטרטיבי מסוג Feistelבן 16 שלבים (סיבובים) שבו  ו- , כלומר, אורך הטקסט הגלוי שווה לאורך הטקסט המוצפן (אורך כל בלוק 64 ביטים), ואורך המפתח הינו 56 ביטים.
* בצפנים מסוג Feistel פונקציית השלב g היא מהצורה הבאה:   
  אם בערך המתקבל בסוף שלב ה-i נסמן את החצי השמאלי והימני ב- ו-  בהתאמה (באורך שווה 32 ביטים) אז עבור פונקציה f כלשהי של שני משתנים מתקיים:  
   כאשר  ו- .
* כל תת מפתח  הוא בחירה של 48 ביטים מתוך המפתח היסודי K (56 ביטים) שעברו תמורה.
* בסוף 16 האיטרציות מוחלפים שני חצאי הבלוק שהתקבל, ומופעלת עליהם התמורה ההופכית לזו שהתחלנו בה. תמורה זאת נקראת Initial Permutation, או בקיצור IP:

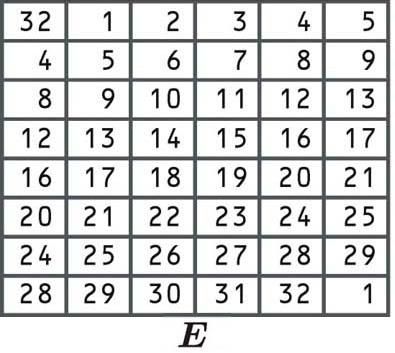


* להלן סקיצה של שלב אחד בהצפנת DES.



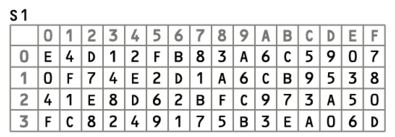
**הפונקציה f (feistel)**

* הפונקציה מקבלת שני קלטים: הבלוק הימיני באורך 32 ביטים, והתת מפתח הנוכחי באורך 48 ביטים ומחזירה פלט בן 32 ביטים.
* פעולת ההרחבה E הופכת את הבלוק הימיני מ-32 ביטים ל-48 ביטים באמצעות שכפול מחצית 16 מהביטים:



* לאחר מכאן מבוצע פעולת XOR בין ההרחבה של הבלוק הימיני לתת מפתח הנוכחי, והפלט מחולק ל-8 תת בלוקים , i=1,2,...,8 ,שכל אחד מהם באורך 6 ביטים.
* כל בלוק  מוזן ל-S-box (Substitution Box) ומחזיר פלט בן 4 ביטים- סה"כ 32 ביטים. להלן דוגמא לחישוב S-box:

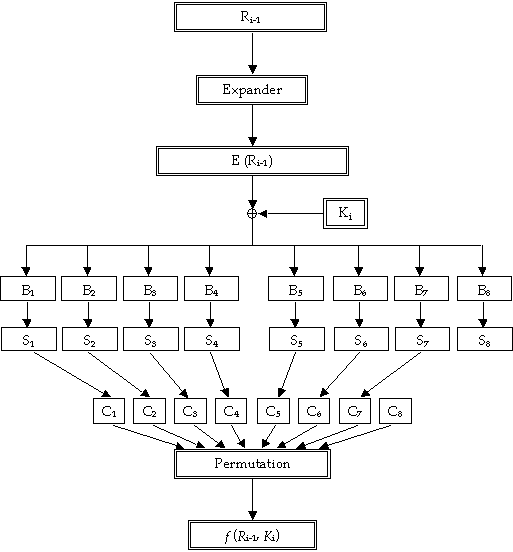
נניח שהקלט הינו 6 ביטים הבאים : 101000.   
הביט הראשון והאחרון נותנים את הערך הבינארי 10, שבמספר שלם הינו 2.   
הארבעה ביטים האמצעיים נותנים את הערך הבינארי 0100, שבמספר שלם הינו 4.   
נבחר (לפי התוצאות שקיבלנו) שורה מספר 2 ועמודה מספר 4, שם מופיע הערך D, אשר בבינארי הינו 1101. ערך זה הינו הערך המוחזר.



* לבסוף, שמונת הפלטים משורשרים לבלוק בן 32 סיביות אשר מועבר לתמורה קבועה P:



* פלט התמורה הוא הפלט הסופי. להלן סקיצה המתארת את תהליך פונקציה f במלואה.



* 1. **בטיחות וחסינות DES**
* הקדמה:   
  כל מרכיבי הצפנת DES הינם לינארים, פרט ל-S-boxes שאינן ליניאריות (ומכאן נובע חוזק צופן זה) בנוסף, רק 16 השלבים המרכזיים תלויים במפתח (בכל שלב בתת מפתח המתאים לו), בעוד ששלוש הפעולות החיצוניות אינן תלויות במפתח ולכן אינן תורמות לבטיחות ההצפנה. מספר חוקרים חששו שה- S-boxes עלולים להכיל "דלת אחורית" אשר הוטמנו ע"י ה- NSA ו-IBM, ויאפשרו לשבור הודעות מוצפנות בקלות, למרות שה-NSA טען שהצופן מאובטח. בדיעבד מסתבר כי התיבות עוצבו באופן כזה שהצופן יהיה עמיד יחסית כנגד קריפטאנליזה דיפרנציאלית (עליה נדבר בהמשך הפרק) ושהשינויים שהתבצעו ע"י ה-NSA ב-S-boxes במשך השנים נועדו לחזק את הצופן כנגד התקפה זו, שהייתה ידועה להם ולמפתחי הצופן ב-IBM משפורסם הצופן.
* תקיפות על DES:   
  ארבעת התקפות על DES הראשונות הר"מ מתוארות ע"פ [3],[4],[5].
  + **התקפת כוח גס (Brute Force)**נקרא גם התקפת חיפוש מפתח ממצה (Exhaustive key search)**.**DES משתמש במפתח סודי באורך 56 סיביות. השיטה הפשוטה היא לנסות לפענח את הבלוק עם כל מפתחות האפשריים, כלומר . המידע שיש לנו על הטקסט הגלוי (לדוגמא אם זה קובץ תמונה, או אותיות באנגלית) יאפשר לנו לזהות את המפתח הנכון ולהפסיק את החיפוש. בממוצע נצטרך לחפש 36 מיליון של מיליארדים של מפתחות, בהנחה שמחשב PC מודרני יכול לבדוק בין 1-2 מיליון מפתחות בשנייה, ולכן ייקח כ-600-1200 שנים למצוא את המפתח בהנחה שמשתמשים ב-PC אחד ולכן התקפה זו לא סבירה (בהמשך נראה שעם התקדמות הטכנולוגיה כבר ניתן לשבור את הצופן בהמצאות התקפה זו בהרבה פחות זמן).
  + **פיתוח מכונה ייעודית לשבירת DES**   
    בשנת 1998 ה-EFF(Electronic Frontier Foundation ) בנה מכונה ייעודית כדי להוכיח לעולם שצופן DES אינו נחשב לאלגוריתם מאובטח יותר. השם של המכונה היה Deep Crack והוא נבנה עם 1536 שבבים ייעודיים בעלות של כ-200,000$. מכונה זה הייתה מסוגלת לבדוק 92 מיליארדי מפתחות בשנייה , ולשחזר את המפתח בתוך 4 ימים. בידיעת התקציב של סוכנויות מודיעין (כגון ה-NSA), היה ברור שניתן להסיק ש-DES אינו מאובטח יותר.
  + **שבירת DES ע"י אשכול ענקי של מחשבי PC**   
    בשנת 1999 התברר שגם לא צריך הרבה כסף כדי לשבור את DES, מספיק קבוצת מתנדבים בעולם עם גישה לאינטרנט. ארגון  Distributed.Net, המתמחה באיסוף וניהול זמן המתנה של מחשב שבר וגילה מפתח DES תוך 23 שעות בלבד, בעזרת יותר מ100,000 של מחשבים של מתנדבים בכל העולם (בעלי מעבדים חלשים עד חזקים ביותר).
  + **התקפת יום הולדת (Birthday Attack)**

התקפה זו מנצלת את תופעת פרדוקס יום ההולדת:

אם בוחרים ערכים בעלי סיכוי שווה מבין \ n אפשרויות, אז החזרות הראשונות תופענה כבר כאשר מספר הערכים הוא מסדר גודל של \ \sqrt{n} , ומכאן מסיקים שהסיכויים ששני מפתחות שונים שנבחרו באקראי יניבו תוצאה זהה ( לאותו טקסט גלוי) הינם גבוהים. באמצעות שימוש בתקיפה זו ניתן להפחית את טווח המפתחות לחיפוש מ  ל-  בממוצע.

* + **קריפטאנליזה דיפרנציאלית (Differential cryptanalysis)**התקפה זו מתוארת כפי שמתואר ב-[6].

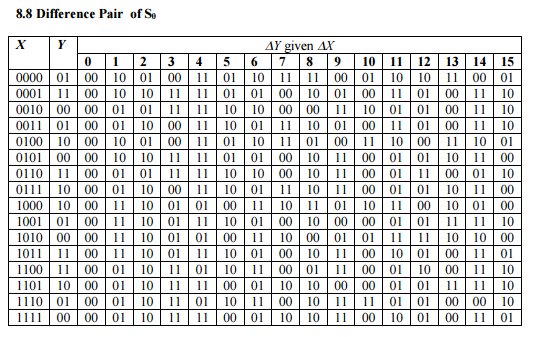
הראשונים לפרסם את הקריפטאנליזה הדיפרנציאלית היו עדי שמיר ואלי ביהם בשנת 1990.

תיאור השיטה:

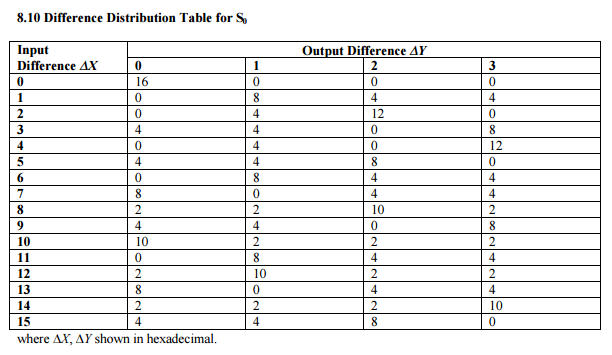
תקיפה מסוג גלוי ידוע בה יכול התוקף להצפין טקסט גלוי על-פי בחירתו. עוסקת בניתוח ההשפעה של שינויים בקלט של פונקציה קריפטוגרפית על הפלט שלה, ובכך למצוא היכן הצופן מתנהג בצורה שאינה אקראית וכך להקטין את מרחב החיפוש של המפתח. התוקף מנסה למצוא קשר סטטיסטי בין (\Delta_X,\Delta_Y) כאשר \Delta_Y = S(X) \oplus S(X \oplus \Delta_X)

S מייצג את המרכיב הלא ליניארי בצופן (S-boxes בצופן DES), כלומר, בודק כיצד משפיע שוני זה על הצופן המתקבל. באמצעות שימוש בקריפטאנליזה דיפרנציאלית ניתן להפחית את טווח המפתחות לחיפוש מ  ל- 2^{47}.   
  
זוגות (\Delta_X,\Delta_Y) של S-Box:  
נתבונן ב-S0 ו-S1. נסמן את הקלט של ה-S-Box ב-X ואת הפלט ב-Y. ה- Difference Pairsשל כל S-Box מסומנות ב- (\Delta_X,\Delta_Y), כאשר  ו- \Delta_Y = S(X) \oplus S(X \oplus \Delta_X).

להלן ה- Difference Pairsשל S0 :



טבלת Difference Distribution:  
להלן טבלאות Difference Distribution של S0 כאשר השורות מתארות את , העמודות מתארות את , והערכים מתארים את מספר המופעים בהינתן ערכי שורה ועמודה.



* ניתן להסיק מטבלאות אלו ערכי קלט ופלט אפשריים בהתחשב בהבדלים ביניהן, ע"י בדיקת הערך המתאים בטבלה. לדוגמא, נניח ש-  ו-  של S0 . מהטבלה ניתן לראות שמספר המופעים הוא 2. מכיוון ש- אז זוגות הפלט בהכרח הן 1 או 3. לאחר מכן ניתן לראות שערך זוגות הקלט המתאים לכך, וכן שהתקיים  הינו 1 או 9. בנוסף, ניתן להסיק מספר ביטים של המפתח.

מאפיינים דיפרנציאליים:

בעזרת מאפיינים אלו ניתן להסיק את התת מפתח אשר משמש לסיבוב האחרון של DES. ראשית, נבנה מאפיים זה בעזרת Difference Pair של S0 ו-S1 :

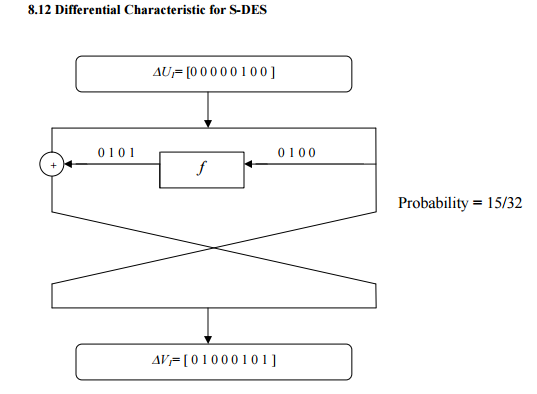


לפי הנ"ל ולפי ההרחבה   

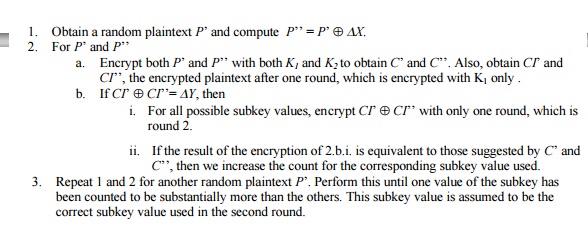

נסיק שהשונות בקלט הינו  
 

לאחר מכן, לפי  והתמורה P ניתן להסיק את השונות בפלט   

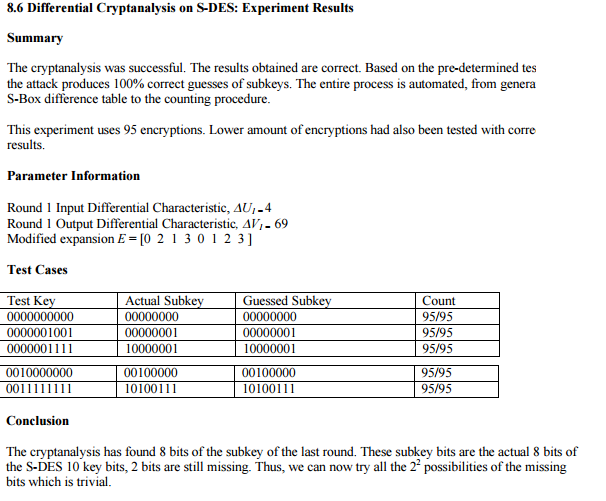

להלן תרשים המתאר תהליך זה לסיבוב 1 :



כעת, בעזרת התהליך הנ"ל שתיארנו, ובעזרת האלגוריתם הבא, ניתן לחלץ מספר ביטים של מידע על המפתח:



ע"פ אלגוריתם זה והפרמטרים הנ"ל, ההתקפה הצליחה לחלץ את כל התת מפתח של סיבוב 2 (8 ביטים של מפתח מתוך ה-10 התגלו ו-2 עדיין חסרים אך ניתן לנסות 4 אפשרויות כדי לגלות מהן):



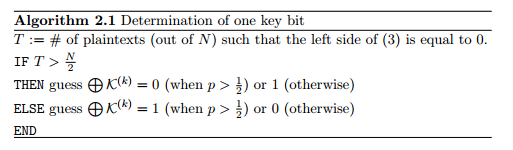
* + **קריפטאנליזה ליניארית (Linear cryptanalysis)**התקפה זו מתוארת כפי שמתואר ב-[7].ב-DES הרכיב היחידי באלגוריתם שאינו לינארי הוא ה-S-BOXES , כפי שתיארנו בפרק 4.כל שאר המרכיבים הינם ליניאריים ופשוטים לניתוח**.**

בשנת 1994 פורסם ע"י היפני מיטסורו מאטסוי לשבירת צופן DES. התקפה זו מסוג התקפת גלוי-ידוע דורשת אחסון של \ 2^{43} זוגות של טקסט גלוי וטקסט מוצפן בהתאמה (כ-GB 64000 ) ולכן אינה נחשבה מעשית בזמנו. במהלך ניתוח הצופן, מחפש התוקף קירוב ליניארי לפעולתו ובאמצעות הצבה של טקסטים ידועים גוזר ערכים מתוך המפתח. מאז פורסמה הפכה השיטה לפופולארית בקרב מנתחי צפנים ועברה שיפורים רבים.

קריפטאנליזה ליניארית מנסה לנצל את אירועי הסתברות גבוהים של ביטויים לינאריים הכוללים ביטים עם טקסט גלוי, טקסט מוצפן ותת מפתח.   
  
תיאור השיטה:   
שימוש קריפטאנליזה ליניארית מורכב משני שלבים. בשלב הראשון מחפש התוקף קירוב ליניארי בין הטקסט הגלוי, הטקסט המוצפן והמפתח בעל קירוב ככל האפשר ל-0 או 1‏. לאחר שנמצא קירוב ליניארי מספק, מציב התוקף במשוואה זוגות ידועים של טקסט גלוי, טקסט מוצפן כדי לחשב מתוכם חלקים מתוך המפתח. בהתאם לטיב הקירוב \ k יש להציב 2^k זוגות כאלה. לאחר שנמצא קירוב לינארי מספק מהצורה : 
P_{i_1} \oplus P_{i_2} \oplus \cdots \oplus C_{j_1} \oplus C_{j_2} \oplus \cdots = K_{k_1} \oplus K_{k_2} \oplus \cdots
  
מציבים בנוסחה זוגות ידועים של (טקסט גלוי, טקסט מוצפן) כדי לגזור את סיביות המפתח. עבור כל זוג המוצב בפונקציה מתקבל ערך כלשהו של המפתח, הערך המופיע יותר פעמים הוא בעל סבירות גבוהה יותר להיות ערך המפתח הנכון.  
בפרויקט מחקר של LASEC הציגו איך הצליחו לשבור מפתח של DES בארבעה ימים, לאחר שיישמו הצפנת DES שגרתית באמצעות שימוש בטכניקות מתקדמות בארכיטקטורת Intel Pentium III אשר מסוגלת להצפין בשיעור של 192 מגה ביט לשנייה על מעבד 666MHz PIII

השגת bit אחד של מידע על המפתח הסודי:  
בהינתן קירוב לינארי יעיל, ניתן להשיג ביט אחד של מידע על המפתח הסודי. הגודל אפסילון מייצג את יעילות של הביטוי הלינארי הנ"ל:



בעזרת האלגוריתם הר"מ, המדדים ה-K נקבעים ע"י הביטוי הלינארי:   


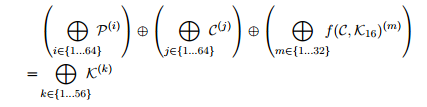
ניתן לראות ששיעור ההצלחה יגדל כאשר מספר זוגות ידועים של טקסט גלוי, טקסט מוצפן יגדל (N במשוואה) או אפסילון יגדל.

נסיק את למה 2.1 (ההוכחה מתוארת במאמר) :

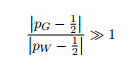
****

השגת מספר רב של ביטים של מידע על המפתח הסודי:

מאטסוי משתמש בקירוב ליניארי היעיל ביותר על n-1 סיבובים (rounds) לצורך השגת יותר מביט אחד של מידע על המפתח הסודי.

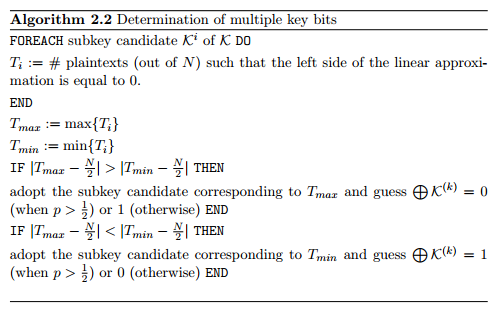


אם נבצע חילוף אחד של תת מפתח שגוי K16, היעילות של הקירוב הליניארי תקטן. עובדה זו צוינה ע"י " wrong key randomization hypothesis":



ההסתברות PG שקירוב ליניארי אם נפענח את הסיבוב האחרון עם התת-המפתח הנכון גדול יותר מההסתברות PW אם נפענח את הסיבוב האחרון עם התת מפתח שגוי.

אלגוריתם 2.2 הינו שיטה לסבירות מקסימאלית של עדכון קירוב ליניארי.

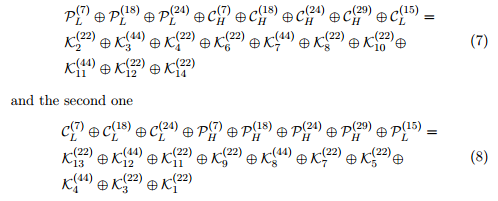


אלגוריתם זה מאחזר בהסתברות הצלחה מסוימת i ביטים שמגיעים מה-תת מפתח התקין וביט אחד על סכום של מספר ביטים במפתח שבונים את החלק הנכון של הביטוי הלינארי.

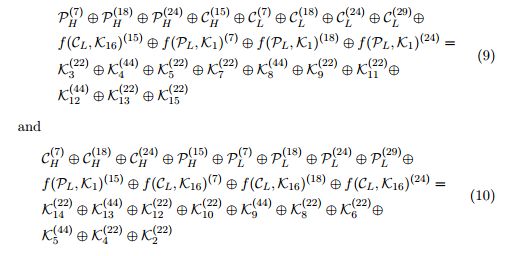
**בעזרת אלגוריתם זה,** מאטסוי הוכיח איך ניתן לשבור DES תוך שימוש ב-  טקסט גלוי ושני קירובים ליניאריים שונים, כל אחד על  אחד. בשיטה זו שוחזרו 14 ביטים מהמפתח, ושאר 42 הביטים במפתח נמצאו ע"י חיפוש ממצה (כוח גס). מאטסוי העריך שהסתברות ההצלחה של תקיפתו הינה  בסיבוכיות  ( לחיפוש כוח גס).

התקפת DES 16 סיבובים:

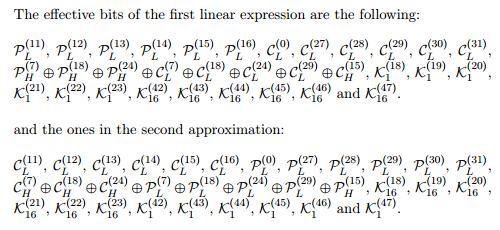
לצורך שבירת DES עם 16 סיבובים, מאטסוי הראה כיצד ניתן לשפר את ההתקפה הנ"ל. הוא עבד עם ביטוי ליניארי על 14 סיבובים של DES. לכל משוואה יש שתי  פעילים (1 ו-5) וכל אחד יכול להחזיר 13 ביטים מהמפתח, 26 ביטים סה"כ. מאטסוי הסיק את שתי הביטויים הליניאריים הטובים ביותר הבאים, אשר מהווים הבסיס המרכזי לתקיפה זו:



נקצה משוואות אלו לסיבוב ה-15 של DES ונקבל את שתי הקירובים הליניאריים הסופיים הבאים:



לאחר מכן, נגדיר את ה-text bits ואת ה-key bits היעילות, אשר משפיעות על החלק השמאלי של הקירוב הלינארי:



לכן ניתן לראות ש- 13 text bits יכולים לשמש להפקת 12 key bits וביט נוסף של הצד הימיני של כל משוואה, ולכ סה"כ משיגים 26 ביטים מהמפתח הסודי משתי המשוואת, תוך שימוש ב-26 ביטים של טקסט.

* בטיחות DES:   
  כפי שמתואר ב-[1],[4],[5], שלושת ההתקפות האחרונות שתוארו אמנם יעילות יותר מהתקפת כוח גס, אך עדיין דורשות כמות גדולה של טקסטים גלויים ומוצפנים על מנת למצוא את מפתח ההצפנה. אולם, עם ההתפתחות הטכנולוגית בעולם מאז פורסמה DES, באמצעות חומרה ייעודית ניתן **לשבור את DES ביום אחד** בלבד, כפי שראינו בתקיפות הנ"ל. יש לציין שתקיפות הנ"ל שבוצעו באמצעות חומרה ייעודית בוצעו בסוף שנות ה-90, וכיום ניתן בהחלט לבנות מכונות מסוג דומה במחירים נמוכים בהרבה ובזמנים טובים יותר במידה ניכרת. ניתן להסיק מכך שחולשתו העיקרית של **DES הינו מרחב מפתחות קט**
  1. **DES2 ו-3DES ובטיחותם**
* הקדמה:   
  כמו שציינו, החולשה העיקרית של DES שהתבררה במהלך השנים הינה מרחב המפתחות הקטן ולכן ניסו להרחיב את מרחב המפתחות תוך כדי המשכת שימוש באלגוריתם DES.   
  נתאר וננתח שיטות אלו כפי שמתואר ב-[1],[3].
* 2DES ובטיחותו:  
  שיטה ראשונה הינה 2DES, או הצפנה כפולה באמצעות DES, שבו הרחבנו את מרחב המפתחות בריבוע ומפתח ההצפנה כפול באורכו (112 ביטים). הגדרה פורמאלית:



התקיפות הנ"ל שתוארו על DES אינן ישימות על 2DES עקב גודל המפתח, אך ישנה תקיפה אחרת אשר מאפשרת להפחית את חיפוש טווח המפתחות, ובכך לבצע התקפת כוח גס באמצעות חומרה ייעודית. **התקפה זו נקראת Meet in the Middle (MITM):**   
התקפת טקסט גלוי ידוע. נניח שהיריב השתמש בהצפנה כפולה עם מפתחות K1 ו-K2, ויש לנו שני זוגות של טקסט גלוי וטקסט מוצפן, כלומר, עבור i=1,2 מתקיים . נבנה טבלה של כל ההצפנות האפשריות של P1 באמצעות כל אחד מהמפתחות. כעת נעבור על כל המפתחות ונפענח את C1 באמצעות כל אחד מהמפתחות ונחפש את התוצאה המתאימה בטבלה.  
בהצפנת DES נאחסן את כל  ההצפנות האפשריות עם מפתחות שונים, נפענח באמצעות כל אחד המפתחות את ההצפנה ונחפש את התוצאה המתאימה בטבלה, ובכך ניתן לצמצם את זמן ההתקפה ל-(ועם שיטות תקיפה הנ"ל אף פחות), ולכן ניתן להסיק שגם מיתן לשבור את הצופן 2DES.

* 3DES ובטיחותו:

שיטה שנייה הינה 3DES, או הצפנה משולשת באמצעות DES, שבו הרחבנו את מרחב המפתחות בריבוע ומפתח ההצפנה כפול באורכו (112 ביטים). חסרון צופן זה הינו איטיותו, אך למרות זאת הוא נמצא בשימוש נרחב בעולם. הגדרה פורמאלית:



חסרון התקיפות הנ"ל שתוארו על DES אינן ישימו על DES עקב גודל המפתח, וכן בשל התקפת MITM גודל המפתח הינו , ולא ניתן לשבירה ע"י התקפת כוח גס.

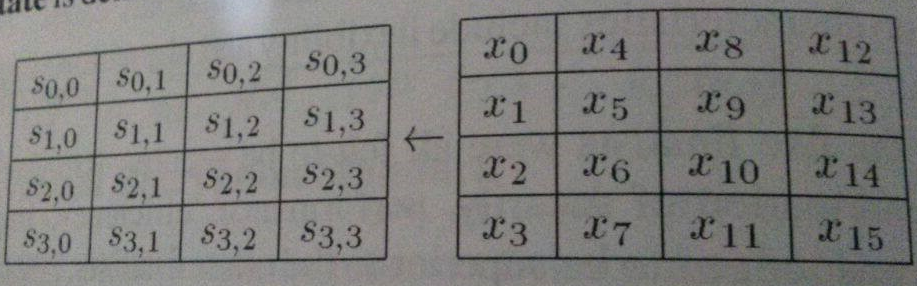
1. **Advanced Encryption Standard (בראשי תיבות AES)**
   1. **רקע היסטורי**ב-1997 המכון הלאומי לתקנים וטכנולוגיה (NIST) התחיל תהליך של חיפוש אלגוריתם הצפנה להחלפת DES. לסיבוב הסופי עלו 5 מועמדים. האלגוריתמים דורגו לפי ניקוד שניתן להם בקטגוריות השונות, ביטחון, יעילות, קלות יישום והטמעה בחומרה.  
      בנובמבר 2000 הוכרז אלגוריתם ריינדל כנבחר, אשר פותח על ידי הקריפטוגרפים הבלגיים יוהאן דאמן ווינסנט ריימן . בנובמבר 2001 הוכרז כתקן הצפנה ובמאי 2002 אושר רשמית ע"י מזכיר המסחר בארה"ב וכן הוכרז כתקן ISO (ארגון התקינה הבינלאומי).
   2. **תיאור AES**

נתאר אלגוריתם זה לפי [1].

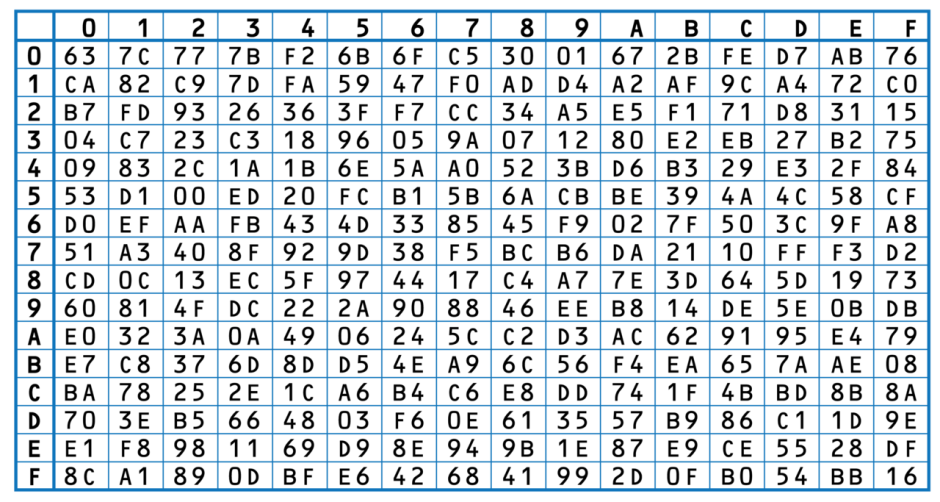
* AES הינו צופן בלוקים סימטרי איטרטיבי מסוג החלפה/תמורה (SPN) שבו  ו-  כאשר b ו-t יכולים להיות באורך 128,192,256 ביטים ומספר השלבים בו הוא 10,12,14 (בהתאם לאורך המפתח). נציג תחילה את תיאור האלגוריתם ואז נסביר על השלבים שבו. תיאור האלגוריתם בפסיאודו-קוד:

  
For i=1 to i=Nr-1 do {  
 s=SubBytes(s);  
 s=ShiftRows(s);   
 s=MixColumns(s);  
  }   
s=SubBytes(s);  
s=ShiftRows(s);  
  
Output y;

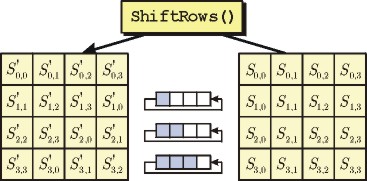
* נתאר את האלגוריתם למקרה שאורך המפתח הינו 128 ביטים.
* המשתנה s מורכב מ-16 בתים מאורגנים בטבלה 4X4 אשר איתחולה הינו באופן הבא, כאשר X הינו הטקסט הגלוי ו-S הינו המצב הנוכחי/ביניים (State):



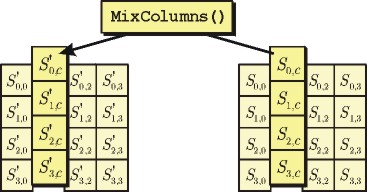
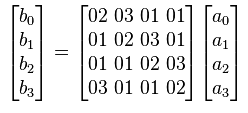
* הפעולה SubBytes: תמורה על אוסף הבתים באופן לא ליניארי לפי ה-S-box. לדוגמא, אם  התוצאה תהיה הערך שנמצא בשורה 5 עמודה 3 שהינו ED.



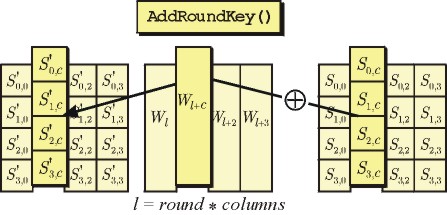
* הפעולה ShiftRows: פעולה זו עושה הזזה שמאלית מעגלית ב-i מקומות על שורה i בטבלה 4\*4, כאשר i מקבל את הערכים 0-3:

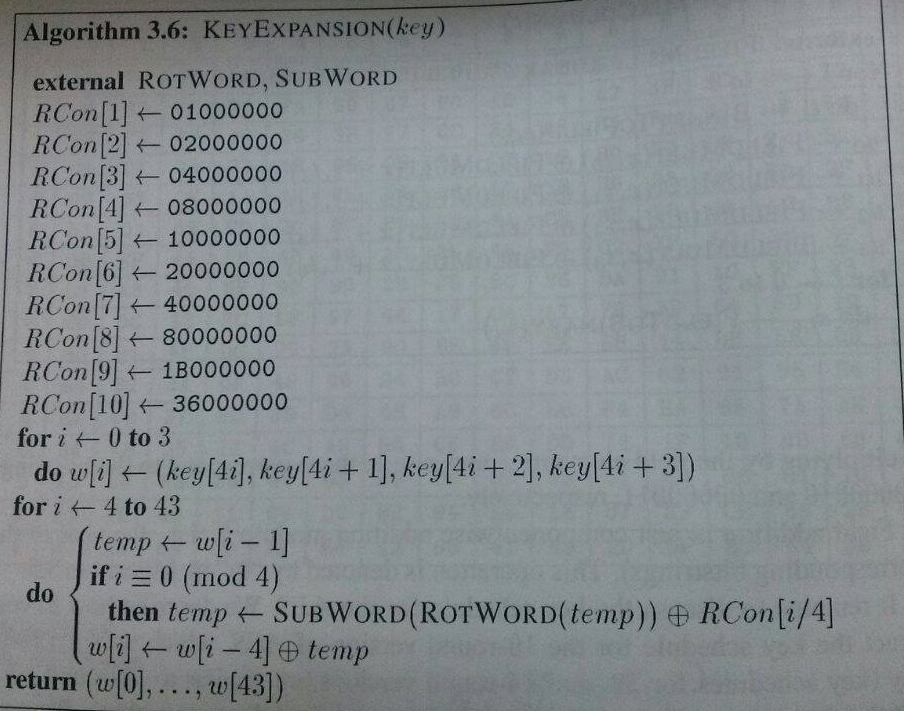


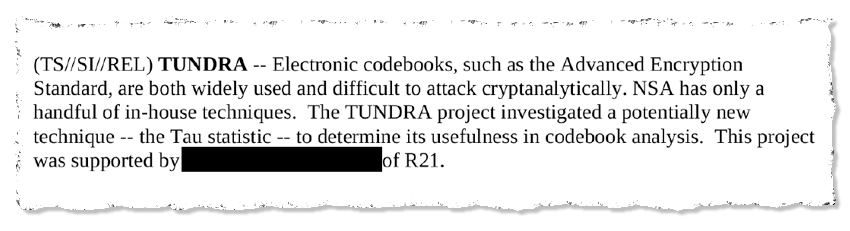
* הפעולה MixColumns: פעולה זו פועלת על עמודות הטבלה. אפשר לתאר פעולה זו ככפל במטריצה   כאשר c הינה מטריצה קבועה ו-a עמודה ב-s:

* טבלת תזמון מפתחות: הערכים  עד  מהווים את התת מפתחות אשר מחושבים מהמפתח היסודי K. מעדכנים את ערכי כל בתי המצב באמצעות חישוב XOR עם מפתח הסבב (round key). מפתחות הסבבים הם פונקציה של מפתח הצופן המסופק על ידי המשתמש. סך כל סיביות המפתח המורחב שווה לגודל הבלוק הנבחר כפול מספר הסבבים ועוד אחד. עבור בלוק של 128 סיביות יהיו 1408 סיביות מפתח מורחב, אותם מחלקים ל-10 מילים לפי הסדר.





* 1. **בטיחות וחסינות AES**
* הקדמה:   
  אחד מהקריטריונים לקבלת אישור לתקן הצפנה של אלגוריתם ריינדל ע"י המכון הלאומי לתקנים וטכנולוגיה (NIST) היה חסינות מפני תקיפות צופן ידועות (לדוגמא ההתקפות שתיארנו בפרק 4.3). אורך המפתח הסודי מתמודד עם תקיפת כוח גס, ולפי מה שידוע כיום, לא ניתן לשבור צופן זה באמצעות תקיפה זו. בנוסף, הצופן פותח כדי להתמודד עם קריפטאנליזה דיפרנציאלית וליניארית ע"י בחירה מושכלת של תיבות ההחלפה (S-box) באופן שלא תהיה להם עקבה דיפרנציאלית או ליניארית,לדוגמא: פעולת היפוך של השדה הסופי בבניית ה-מפיק שהקירוב ליניארי והשונות בטבלאות ההתפלגות שמשמעותה שהערכים קרובים לאחידות. זה מספק אבטחה נגד התקפות ליניאריות ודיפרנציאליות. כמו כן, הטרנספורמציה הליניארית MixColumns גורמת שיהיה בלתי אפשרי למצוא התקפות ליניאריות ודיפרנציאליות שכרוכים ב- פעילים. ניתן לסכם ש- **AES מאובטח נגד כל המתקפות known attacks** , נכון לתאריך פרסומו.
* תקיפות על AES:
  + **attack eXtended Sparse Linearization**או בקיצור תקיפת XSL , כפי שמתואר ב-[8], הינה תקיפה שפותחה בשנת 2002 ע"י הקריפטוגרפים ניקולס קורטויז ויוסף פייפרציק ולטענתם מסוגלת לשבור את AES בזמן קצר יותר באופן משמעותי מתקיפת כוח גס. ההתקפה פועלת על ידי גזירת מערכת משוואות ריבועיות מהצופן, שהן פונקציה של הטקסט המקורי, הטקסט המוצפן והמפתח.  
     הם הציעו פתרון באמצעות טכניקה שהמציאו לצמצום מספר הנעלמים שנקראת eXtended Sparse Linearization המסתמכת על עבודתם של שמיר וקיפניס. אולם הסתבר שהשיטה דורשת משאבים עצומים ואינה יעילה מכוח גס כפי שנטען בתחילה על ידי המפתחים, לכן הינה נחשבת תיאורטית כיום.
  + **Related-key attack**כפי שמתואר ב-[9] , הינה תקיפה שפורסמה ביולי 2009 ע"י הקריפטוגרפים אלכס בריוקוב ודימטרי חובראטוביץ על גרסאות 192 ביט ו-256 ביט. התקפה מסוג זה מניחה שהתוקף מסוגל לבחור מפתחות שיש ביניהם קשר או יחס כלשהו. ההתקפה מתמקדת בתהליך הרחבת המפתח הפשוט יחסית של AES בגרסאות AES-192 ו-AES-256 והגיעה לסיבוכיות של . מכיוון שהנחה זאת אינה סבירה והמפתחות ב-AES נבחרים באקראי, התקפה זאת לא סבירה.  
    התקפה דומה שהמציאו המפתחים האמורים יחד עם שמיר, דונקלמן וקלר, כנגד AES-256 מצליחה לחשוף את המפתח רק עם שני מפתחות קשורים, בזמן של 2^{39} בתשעה סבבים, 2^{45} בעשרה סבבים ו-2^{70} ב-11 סבבים. אף אחת מההתקפות לא יעילה כנגד AES במלוא הסבבים.
  + **Biclique attack**כפי שמתואר ב-[10], הינה סוג של תקיפת MITM שפורסמה בשנת 2011 ע"י הקריפטוגרפים בוגדנוב, חובראטוביץ' ורכנברג. biclique הוא סוג מיוחד של גרף דו-צדדי שבו כל קודקוד של הסט הראשון מחובר לכל קודקוד של הסט השני. תקיפה זו מנצלת את מבנה biclique להרחיב את מספר הסיבובים האפשרי שהותקפו ע"י MITM. התקפה זו הינה טובה יותר מכוח גס: ל- AES-128צריך  פעולות, ל- AES-192מצריך  פעולות ול- AES- 256 מצריך  פעולות. החוקרים חישבו שההתקפה הכי טובה באמצעות שיטה זו על - AES-128 דורשת  ביטים של מידע (כמות עצומה של מידע), ולכן זו התקפה תיאורטית ואינה יכולה לשבור את AES (כיום).
  + **תקיפת AES ע"י ה-NSA**כפי שמתואר ב-[11], אחת מחשיפות אדוארד סנודן של מסמכי ה-NSA חשפה ניסיונות לשבור צופן AES באמצעות  tau statisticאך לא ידוע אם ניסיונות אלו הצליחו.
  + **תקיפת ערוץ צדדי (Side-channel attack)**

כפי שמתואר ב-[12], הינה תקיפה לא ישירה על צופן AES, כלומר, בהתקפה זו לא מנסים לשבור את צופן AES אלא לנצל חולשות באופן יישומו במערכת ולנסות להשיג מידע אודות הצופן ו/או המפתח.  
באפריל 2005, פרסם דניאל ברנשטיין התקפת תזמון (cache timing attack)‏ שהצליחה לפרוץ לשרת ייעודי שיישם הצפנת AES כחלק ממערכת SSL. השרת נבנה כך שיאפשר חשיפה של מידע תזמון רב ככל האפשר. הסיבה לפרצה נובעת מהנדסת האלגוריתם והמבנה האלגברי הייחודי שלו, עובדה המקשה על כתיבת קוד בטוח (שפועל בזמן אחיד) למרות שהחולשה קיימת גם באלגוריתמים נוספים. עדי שמיר וחוקרים ממכון ויצמן, פרסמו מספר התקפות תזמון דומות כנגד AES, אחת מהן הצליחה לחשוף את המפתח כולו אחרי 800 כתיבות לזיכרון בלבד בתוך מספר מילישניות. יש לציין כי התקפות האמורות התבצעו על שרת ייעודי, באופן שאפשר גישה ישירה לתוקף, תנאי שאינו מעשי דרך רשת האינטרנט.

* בטיחות AES:  
  **צופן AES נחשב כיום לצופן סימטרי הבטוח והחסין ביותר**. תיארנו מספר התקפות שהינן תיאורטיות בלבד ולא מצליחות לשבור את AES. אולם יתכן שארגוני ביטחון ממשלתיים כגון ה-NSA הצליחו לשבור את AES ושומרים מידע זה לעצמם לצרכי ביטחונם כפי שעשו במקרים אחרים בעבר (ידוע לדוגמא שרעיון מפתח הפומבי היה ידוע ל-NSA הרבה לפני פרסומו). בנוסף, נראה שעולם חדש של תקיפות מתחיל **- תקיפות ערוץ צדדי**: במקום לנסות לשבור את הצופן (כפי שראינו כנושא קשה מאוד), ניתן לנצל חולשות באופן יישום הצופן ובכך להשיג מידע חשוב עליו.

1. **סיכום ומסקנות**

בעבודה זו הצגנו את שתי אלגוריתמי ההצפנה הסימטרי DES ו-AES.

ניתן להגיד בוודאות ש-DES **אינו** חסין וניתן לשבירה די בקלות כיום עקב אורך מפתח קצר. אולם ראינו שבוצע שיפור לאלגוריתם זה בשם 3DES אשר חסין ולא ידוע כיום על תקיפה לשבירתו (לפחות לא בפומבי).

אלגוריתם הצפנה AES, אשר החליף את DES ב-NIST בשנת 2001 נבנה כדי להתמודד עם התקפיות שהיו ידועות על DES. במשך 15 שנה מפרסומו התבצעו ניסיונות והתקפות שונות לשבירתו ללא הצלחה, וניתן להגיד שכיום **AES הינו חסין ובטוח**.

אך ראינו סוג התקפה יחסית חדש בעולם - **תקיפת ערוץ צדדי** שבה במקום לנסות לשבור את הצופן (שנחשב קשה ביותר עד ללא אפשרי), מנסים לנצל חולשות באופן יישומו במערכת ולנסות להשיג מידע אודות הצופן ו/או המפתח.

כיום, ההתפתחות הטכנולוגית בעולם הינה מהירה בצורה יוצאת דופן, ויתכן שבעתיד גם יצליחו לשבור את AES, אך נראה שהעולם שם דגש על תקיפות ערוץ צדדי שהינן יותר אפשריות וקלות.

1. **רשימה ביבליוגרפית**

[1] Cryptography Theory And Practice, Third Edition, Douglas R.Stionson.

### [2] Cryptographic Attacks and Countermeasures, PCcare, security page. link: https://sites.google.com/a/pccare.vn/it/security-pages/cryptographic-attacks-and- countermeasures.

[3] New Comparative Study Between DES, 3DES and AES within Nine Factors,

Hamdan.O.Alanazi, B.B.Zaidan, A.A.Zaidan, Hamid A.Jalab, M.Shabbir and Y. Al-Nabhani   
 MARCH 2010, Journal CoRR

[4] Break Des in less than a single day, **SciEngines** (2009), link:   
 http://www.sciengines.com/company/news-a-events/74-des-in-1-day.html

[5] Six ways to break DES by Pascal Junod, LASEC- Security and cryptography Laboratory. The link: http://lasec.epfl.ch/memo/memo\_des.shtml

[6] Cryptanalysis of S-DES, [K. S. Ooi](http://dblp.uni-trier.de/pers/hd/o/Ooi:K=_S=), Brain Chin Vito,  IACR Cryptology ePrint Archive 2002.

[7] Linear Cryptanalysis of DES, Diploma Thesis ,Pascal Junod, crypto journal . The link:   
 http://crypto.junod.info/lincrypt.pdf

[8] An Analysis of the XSL Algorithm, Carlos Cidand Gaetan Leurent, ASIACRYPT 2005.

[9] Related-key Cryptanalysis of the Full AES-192 and AES-256, Alex Biryukov and Dmitry Khovratovich,   
 [ASIACRYPT 2009](http://dblp.uni-trier.de/db/conf/asiacrypt/asiacrypt2009.html#BiryukovK09).

[10] Biclique Cryptanalysis of the Full AES, Andrey Bogdanov , Dmitry Khovratovich, and Christian   
 Rechberger, [ASIACRYPT 2011](http://dblp.uni-trier.de/db/conf/asiacrypt/asiacrypt2011.html#BogdanovKR11)

[11] Prying Eyes: Inside the NSA's War on Internet Security By SPIEGEL Staff, December 28, 2014, the link: http://www.spiegel.de/international/germany/inside-the-nsa-s-war- on-internet-security-a-1010361.html

[12] Improved Algebraic Side-Channel Attack on AES, Mohamed Saied Emam Mohamed , Stanislav   
 Bulygin, Michael Zohner, Annelie Heuser and Michael Walter.

 J. Cryptographic Engineering   
  HOST 2012  
  IACR Cryptology ePrint Archive 2012

1. **נספח - מושגים כלליים**
2. **המכון הלאומי לתקנים וטכנולוגיה:**The National Institute of Standards and Technology, בראשי תיבות NIST, הינו מכון תקנים ורגולציה אמריקאי, אשר מטרתו לקדם את ארה"ב ע"י חדשנות ותחרותיות בנושאי תקנים, מדע וטכנולוגיה.
3. **International Business Machines (או בקיצור IBM):**תאגיד רב עולמי ואחת החברות הגדולות והוותיקות בעולם בתחום המחשבים.
4. **הסוכנות לביטחון לאומי (National Security Agency):**

בראשי תיבות NSA,  ארגון הביון הממשלתי של ארצות הברית, האחראי על מודיעין אותות - מעקב אחר אותות אלקטרוניים והאזנה להם, פיתוח דרכי הצפנה ופענוח אותות ועוד.