ממן 12

1. ידוע כי DES(x,K)=DES'(x',K') , נשתמש במידע זה על מנת לעשות חיפוש ממצה למפתח.

נניח כי הטקסט הגלוי והמוצפן מוצגים בעזרת ייצוג בינארי. נבצע את הפעולות הבאות:

1. ניקח טקסט גלוי x ונצפין בעזרת DES עם המפתח K שאותו נבחר באקראי, כלומר DES(x,K) ונקבל את הטקסט המוצפן C.
2. ניקח את הטקסט הגלוי x וניקח את x' (כלומר ניקח את x ונבצע עליו את הפעולה XOR עם {1}|x| ).
3. נצפין את x' בעזרת DES עם כל המפתחות האפשריים (256 מפתחות),כלומר DES(x',Ki) כאשר i בתחום בין 1 ל 256 .
4. קיבלנו Ci טקסטים מוצפנים אפשריים מתאימים ונבצע על כל אחד מהם את הפעולה משלים (כלומר XOR עם 1-ים) ואותם נשמור. כלומר הגענו ל DES'(x',Ki)=Ci' שאותם נשמור במערך כאשר האינדיקס הוא Ki.
5. בלי הגדרת הכלליות נעבור על החצי הראשון של המערך, ונבדוק האם Ci'==C ,עבור אותו אינדקס המקיים את השיוויון הוא המפתח בצורת המשלים שלו שחיפשנו, כלומר מצאנו את האינדקס Ki שהוא K' . נבצע XOR על K' עם 1-ים ונקבל את המפתח K.

יש לציין שסעיף א' לא בהכרח דרוש, נוכל להסתפק בטקסט גלוי x וטקסט מוצפן C נתונים ונמשיך ישירות לסעיף ב'. החיפוש אחר המפתח אכן דורש מעבר על 255 מפתחות, ניצלנו מהנתון את העובדה שתכונת פעולת המשלים עבור ייצוג בינארי "חוסכת" לנו לעבור על עוד 255 מפתחות.

1. נקטלג את הבניות הבאות, בהינתן שהיריב יודע את הבנייה אך לא את המפתח:
2. הבנייה DES(x,K1⨁K2) יכולה להיות שקולה ל DES וכן יכולה להיות שקולה ל DES2 תלוי במציאת המפתח. עבור DES- מכיוון שמרחב המפתחות חסום על ידי 256 מפתחות ופעולת ה XOR סגורה תחת ייצוג בינארי נקבל בעצם ש K1⨁K2הוא בעצם מפתח K ממרחב המפתחות ולכן שקול להצפנה DES(x,K) מבחינת היריב. כיוון שמבחינתו אותו מעניין המפתח ולא שני המפתחות שיתנו לנו את המפתח אם נפעיל עליהם את פעולת XOR . לפיכך, יהיה לפחות מפתח אחד שייתן את אותו טקסט מוצפן לטקסט גלוי אבל אין צורך למצוא את כלל המפתחות המתאימים אם הם נותנים את אותה התוצאה כמו מפתח יחיד. עבור DES2 - במקרה וכן נרצה למצוא את K1 ואת K2 אז נצטרך למצוא עבור כל מפתח K איזה מפתחות מרכיבים אותו כלומר יהיה חיפוש של 256\*256 כלומר 2112 מפתחות ומפה נקבל שהבנייה תהיה שקולה ל DES2.
3. DES(x⨁K1, K1) שקולה לDES רגיל, מכיוון שפעולת ה XOR סגורה תחת ייצוג בינארי ולכן x⨁K1  מוכל במרחב הטקסט הגלוי החסום על ידי 264 ביטים ונוכל לסמן אותו כטקסט גלוי x2  . מכאן שההצפנה כביכול תראה DES(x2,K1), כמו כן חיפוש אחר המפתח K­1 ידרוש חיפוש רק של 256 מפתחות, עבור כל מפתח אפשרי נבצע את הפעולה XOR עם הטקסט הגלוי ולאחר מכן נבצע את DES עם אותו K1 .
4. הבנייה DES(x,K1) ⨁K1 שקולה לDES רגיל, מכיוון שחיפוש אחר המפתח K­1 ידרוש חיפוש רק של 256 מפתחות, עבור כל מפתח אפשרי נבצע DES ועל התוצאה נבצע את הפעולה XOR עם אותו מפתח ונשווה בין הטקסטים המוצפנים.
5. הבנייה DES(DES(x,K1),K1') שקולה לDES רגיל מכיוון ש K1' שקול ל K1 XOR עם 1-ים ולכן פעולה זו מהירה מאוד. עבור כל מפתח נבצע DES על טקסט הגלוי ועל התוצאה נבצע DES עם ההופכי של המפתח (מציאת ההופכי היא פעולה מהירה) ולאחר מכן נשווה את הטקסט המוצפן. בסהכ נעבור רק רשימת מפתחות אחת ולכן מספר המפתחות מוגבל ל 256 מפתחות.
6. הבנייה DES(DES(DES(x,K1),K1'),K1) שקולה לDES , כפי שהסברנו בסעיף הקודם הבנייה DES(DES(x,K1),K1') שקולה לDES רגיל ועל כן הצפנת הפלט בעזרת DES עבור אותו מפתח תיתן עדיין מעבר רק על מספר האפשרויות שיש למפתח שהוא 256 מפתחות.

א)החסרונות של המערכת:

1. התקפת Brute force-מרחב המפתחות קטן בהרבה ביחס למפתח רגיל של הצפנה DES. המשתמש בוחר סיסמא K בעלת 8 אותיות באנגלית, באנגלית יש 26 אותיות, גם אם נייצג כל אות עם מספר בינארי עם 5 ביטים נקבל מרחב מפתחות הקטן בהרבה מ 256מפתחות ולכן נצליח למצוא מהר יחסית את המפתח, ההצפנה 60 פעם לא מגדילה את הכוח מעבר לDES.
2. התקפת מילון- מכיוון שהמשתמש בוחר הצפנה בעזרת אותיות באנגלית, נוכל להשתמש בשילובים שונים של מילים נפוצות כגון password על מנת להיכנס אל המערכת. אם ההצפנה המתקבלת תהיה בקובץ הסיסמאות אז המערכת תאשר את המשתמש ונוכל להתכנס, ברגע שנכנס יהיה לנו גישה לקובץ.
3. התקפת צד שלישי- מכיוון שלכל המשתמשים יש גישה לקובץ, כל משתמש יוכל להכנס מאיזה יוזר שהוא רוצה על ידי כך שרשום מי היוזר ויעשה פענוח לפי הנוסחה .
4. מערכת איטית, הצפנה 60 פעם של DES
5. לתוקף יש גישה לקובץ הסיסמאות ולכן יוכל לבחור באופן אקראי את אחד מ N המשתמשים הקיימים. מרחב המפתחות קטן כך שאם המשתמש בוחר סיסמא K בעלת 8 אותיות באנגלית, מרחב המפתחות יהיה 268 מפתחות שהוא קטן בהרבה מDES (גם בייצוג בינארי כאשר כל אות תיהיה 5 ביטים). מכאן שעבור אותו משתמש שבחר יעשה Brute force על 268 מפתחות.
6. שינוי ההצפנה מ60 פעמים ל600 תאט בערך את התוקף פי 10 ותאט את המערכת בכללי, חוץ מהאטה כזאתי מבחינת המרחב המפתחות שעל התוקף לדגום נשאר אותו הדבר ולכן לא תגדיל מבחינה משמעותית את החוזק שלה.
7. כאשר כל תתי המפתחות שווים פעולת ההצפנה והפענוח תהיה אותה הפעולה, ההצפנה של DES תהיה זהה לפעולת XOR, כאשר נפעיל את ההצפנה פעמיים בעצם נקבל את הטקסט הגלוי עצמו .
8. המפתחות אשר עבורם כל תתי המפתחות שווים הם לדוגמא:
   * + 1. 0x0101010101010101
       2. 0xFEFEFEFEFEFEFEFE
       3. 0xE0E0E0E0F1F1F1F1
       4. 0xF1F1F1F1E0E0E0E0