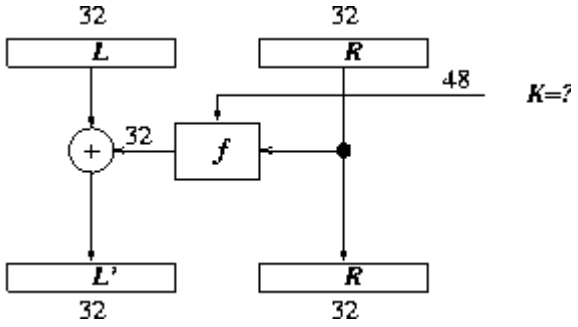
עמוס ביימל **9.4.02**

קריפטוגרפיה: תרגיל 2

הגשה: יום ב' 29/04/02 בהרצאה. ההגשה בזוגות.

שאלה 1

בשאלה זו נראה איך לשבור שלב אחד של DES. נעסוק במערכת הקריפטוגרפית המצוירת לעיל, כאשר f היא הפונקציה שבה משתמשים ב- DES. כלומר, מדובר בשלב אחד של DES כאשר כל "הספיחים" כגון IP וההצלבה סולקו.

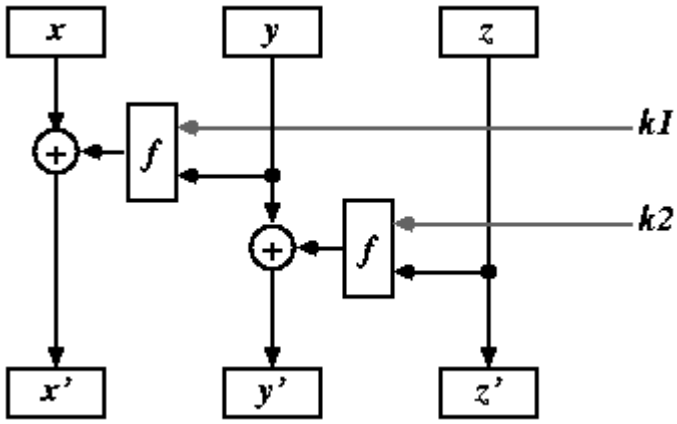


נתון זוג קלט-פלט של המערכת (M,C) כאשר $M=(L,R)$ ו- $C=(L',R)$. כלומר, מדובר ב- Known Plaintext Attack, כאשר מנסים למצוא את המפתח K.

1. הסבירו מדוע הפלט של כל קופסת-S ידוע.
2. בהינתן ארבעת הביטים בפלט של S_1, כמה אפשרויות יש לצירוף של ששת הביטים בקלט ל- S_1 שיצרו אותם?
3. כמה אפשרויות יש לצירוף של ששת הביטים של K המשתתפים ביצירת הצרופים האלה בקלט ל- S_1?
4. מה מספר האפשרויות שנותרו למפתח K?

שאלה 2

עיינו ברשת:



הקלטים x,y,z הם מחרוזות בינאריות באורך n, והפעולות דומות לפעולות ב- DES. בתשובתכם אין להסתמך על תכונות f. נסמן ב- Π את ההעתקה המעתיקה את (x,y,z) ל- (x',y',z').

1. הוכיחו כי Π^4 היא העתקת הזהות. (Π^4 היא ההעתקה המתקבלת ע"י הפעלת Π ארבע פעמים.)
2. האם Π היא חד-חד ערכית ועל? יש לנמק את התשובה.
3. נסמן ב- Θ את ההעתקה $\Theta(x,y,z)=(y,z,x)$. הוכיחו כי Θ^3 היא העתקת הזהות.
4. בונים מערכת הצפנה ע"י $\Pi_3\Theta\Pi_2\Theta\Pi_1$, כאשר ב- Π_j משתמשים במפתחות $k1_j$ ו- $k2_j$. (כלומר, במערכת ההצפנה מפעילים תחילה את Π_1, אח"כ את Θ, וכן הלאה.) הראו כיצד לפענח הודעות במערכת זו.

שאלה 3

שאלה זו מתייחסת למערכת DES כפי שתוארה בכיתה.

סעיף א

הראו כי לכל מפתח $k\in\{0,1\}^{56}$ קיימות בדיוק 2^{32} הודעות $m\in\{0,1\}^{64}$ כך ש- $L_8=R_8$, כאשר L_8 ו- R_8 הם תוצאת הפעלת 8 השלבים הראשונים של DES על ההודעה m תחת המפתח k.

סעיף ב

הוכיחו כי קיימות לפחות 2^{32} הודעות $m\in\{0,1\}^{64}$ כך ש- $\text{DES}(m,0^{56})=m$.

שאלה 4

נתון זוג M_1,C_1 כאשר $C_1=\text{DES}(M_1,\kappa)$ עבור מפתח κ לא ידוע. התקפת חיפוש ממצה מחפשת את κ על ידי מעבר על כל המפתחות עד שנמצא מפתח $k\in\{0,1\}^{56}$ כך ש- $C_1=\text{DES}(M_1,k)$. בהסתברות גבוהה עבור M ו- C נתונים קיים לכל היותר מפתח k יחיד כך ש- $C=\text{DES}(M,k)$ ולכן $k=\kappa$. התקפה זו דורשת 2^{56} הפעלות של DES.

כדי לחזק את DES כנגד התקפת חיפוש ממצה הוצאו שתי השיטות הבאות:

$$\text{DESV}(M,k,k_1)=\text{DES}(M,k)\oplus k_1$$

$$\text{DESU}(M,k,k_1)=\text{DES}(M\oplus k_1,k)$$

כאשר $k\in\{0,1\}^{56}$ ו- $k_1\in\{0,1\}^{64}$.

סעיף א

הראו כיצד מפענחים הודעות ב- DESV ו- DESU כאשר k_1 ו- k נתונים.

סעיף ב

נתונים כעת שתי זוגות הודעות M_1,C_1 ו- M_2,C_2 כאשר $C_1=\text{DESV}(M_1,\kappa,\kappa_1)$ ו- $C_2=\text{DESV}(M_2,\kappa,\kappa_1)$ עבור מפתחות κ ו- κ_1 לא ידועים. הראו איך למצוא את κ ו- κ_1 על ידי התקפה הדורשת $2^{56}\cdot 2$ הפעלות של DES. הסתמכו על העובדה כי עבור M_1,M_2 ו- Δ נתונים, בהסתברות גבוהה קיים לכל היותר k יחיד כך ש-

$$\text{DES}(M_1,k)\oplus\text{DES}(M_2,k)=\Delta.$$

סעיף ג

הראו כיצד לבצע התקפה דומה עבור DESU. כלומר, נתונים כעת שתי זוגות הודעות M_1,C_1 ו- M_2,C_2 כאשר $C_1=\text{DESU}(M_1,\kappa,\kappa_1)$ ו- $C_2=\text{DESU}(M_2,\kappa,\kappa_1)$ עבור מפתחות κ ו- κ_1 לא ידועים. הראו איך למצוא את κ ו- κ_1 על ידי התקפה הדורשת $2^{56}\cdot 2$ הפעלות של DES.