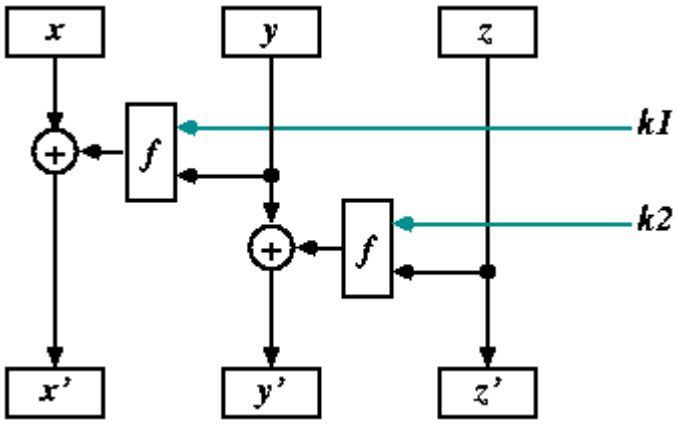
14/11/2012

קריפטוגרפיה: תרגיל 2

הגשה: יום ד' 28/11/12 ב- 16:10 בהרצאה. ההגשה בזוגות או יחידים.

שאלה 1

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').

סעיף א

הוכיחו כי Π^4 היא העתקת הזהות. (Π^4 היא ההעתקה המתקבלת ע"י הפעלת Π ארבע פעמים.)

סעיף ב

האם Π היא חד-חד ערכית ועל? יש לנמק את התשובה.

סעיף ג

נסמן ב- Θ את ההעתקה $\Theta(x,y,z)=(y,z,x)$. הוכיחו כי Θ^3 היא העתקת הזהות.

סעיף ד

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 2

סעיף א

עבור מחרוזת בינארית A, נסמן ב- $\bar{A}$ את המחרוזת המשלימה (כלומר, המחרוזת בה כל אפס מוחלף באחד ולהפך). הוכיחו כי $\mathrm{DES}(\bar{m},\bar{k}) = \overline{\mathrm{DES}(m,k)}$. הסתמכו על העובדה כי המפתח k_i בכל איטרציה הוא תת-קבוצה של הביטים של המפתח k.

סעיף ב

הראו, בעזרת סעיף א, איך לבצע התקפת חיפוש ממצה על DES המשתמשת ב 2^{55} הפעלות של DES. איזו סוג התקפה תיארתם?

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- $DES(m,0^{56})=m$.

שאלה 4

סעיף א

בסעיף זו תראו איך לשבור גרסה של מערכת הצפנה דמוית AES עם סיבוב אחד. ליתר דיוק, נעסוק במערכת הקריפטוגרפית המתוארת לעיל. הראו איך במערכת זאת בהינתן הודעה M כלשהי והצפנה שלה C, ניתן בצורה יעילה לחשב את המפתח k_1.

Simple AES

Input:
in: Message
k_1: key
Begin
state = in
state = SubBytes(state)
state = ShiftRows(state)
state = MixColumns(state)
state = AddRoundKey(state, k_1)
Output:

בסעיפים הבאים תראו איך לשבור מערכת הצפנה דמוית AES עם 3 סיבובים כאשר הורדנו את הפונקציה **`MixColumns`**. ליתר דיוק, נעסוק במערכת הקריפטוגרפית המתוארת לעיל.

Simple AES

Input:
in: Message
k_1, k_2, k_3: keys
Begin
state = in
For i = 1 **to** 3
state = SubBytes(state)
state = ShiftRows(state)
state = AddRoundKey(state, k_i)
Endfor
out = state
End

סעיף ב

נאמר כי ביט של מפתח משפיע על ביט פלט אם שינוי של הביט במפתח ללא שינוי ביטים אחרים במפתח או בהודעה יכול לשנות את ביט הפלט. נסתכל על ביט כלשהו בפלט של Simple AES. כמה ביטים של המפתח משפיעים על הביט הזה לכל היותר?

סעיף ג

הניחו כי בהינתן זוג קלטים in ו in' ופלטים out ו out' קיימת לכל היותר שלשת מפתחות k_1, k_2, k_3 אחת המעתיקה את הקלטים הנ"ל לפלטים המתאימים. תארו התקפה יעילה ככל האפשר המקבלת קלטים in ו in' ואת הפלטים המתאימים להם out ו out' ומוצאת את המפתחות k_1, k_2, k_3. מהי סיבוכיות ההתקפה שתיארתם?

שאלה 5

יהיו m_1 ו- m_2 טבעיים כך ש-$\gcd(m_1, m_2) = p$, כאשר p ראשוני ו- p איננו מחלק את $\frac{m_1}{p}$ ו את $\frac{m_2}{p}$. נסתכל על מערכת המשוואות:

$$x \equiv a \ (mod\ m_1)$$
$$x \equiv b \ (mod\ m_2)$$

סעיף א

הוכיחו כי אם $a \not\equiv b \ (mod\ p)$ אזי אין למערכת פתרון.

סעיף ב

הוכיחו כי אם $a \equiv b \ (mod\ p)$ אזי למערכת קיים לפחות פתרון אחד.
רמז: התבוננו במערכת המשוואות הבאה:

$$x \equiv a \ (mod\ p)$$
$$x \equiv a \left(mod \frac{m_1}{p}\right)$$
$$x \equiv b \left(mod \frac{m_2}{p}\right)$$

הערה: בפתרון עליכם גם להסביר מדוע זאת מערכת משוואות לגיטימית.

סעיף ג

הוכיחו כי אם $a \equiv b \ (mod\ p)$ אזי מספר הפתרונות ב- $\mathbb{Z}_{m_1 \cdot m_2}$ של מערכת המשוואות הוא p.