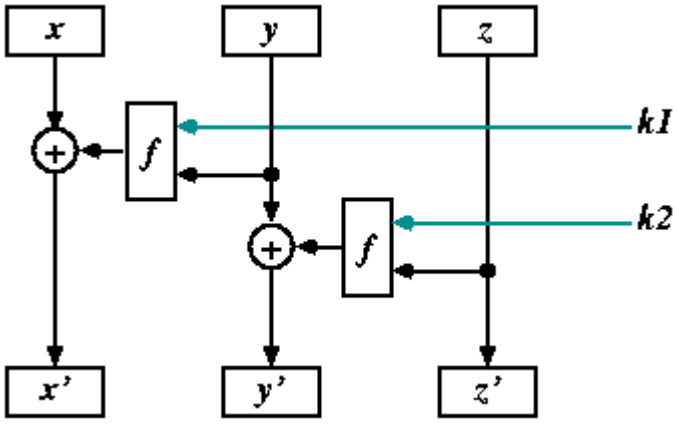
13/11/2013

קריפטוגרפיה: תרגיל 2

הגשה: יום ד' 27/11/13 ב- 14:10 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

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

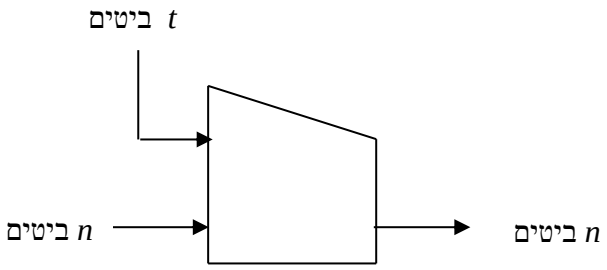
נאמר כי ביט של מפתח משפיע על ביט פלט אם שינוי של הביט במפתח ללא שינוי ביטים אחרים במפתח או בהודעה יכול לשנות את ביט הפלט. נסתכל על ביט כלשהו בפלט של Simple AES. כמה ביטים של המפתח משפיעים על הביט הזה לכל היותר?

סעיף ג

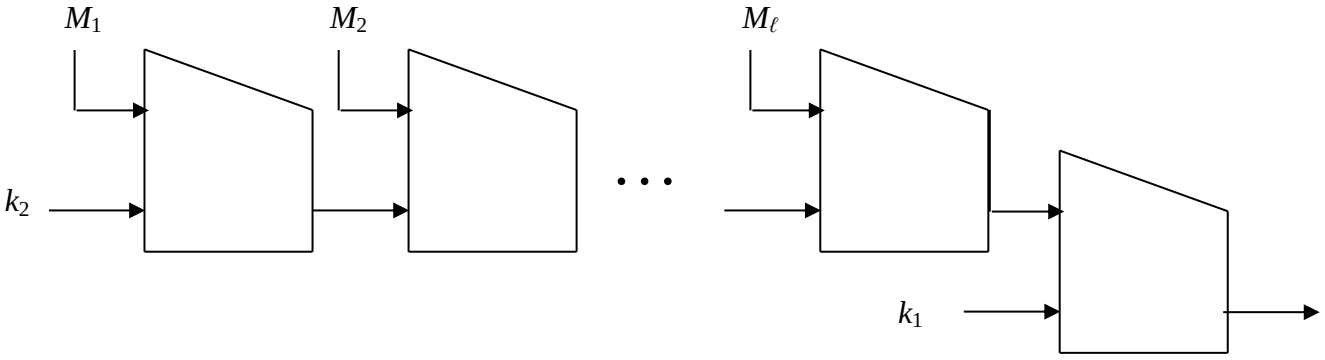
הניחו כי בהינתן זוג קלטים in ו in' ופלטים out ו out' קיימת לכל היותר שלשת מפתחות k_1, k_2, k_3 אחת המעתיקה את הקלטים הנ"ל לפלטים המתאימים. תארו התקפה יעילה ככל האפשר המקבלת קלטים in ו in' ואת הפלטים המתאימים להם out ו out' ומוצאת את המפתחות k_1, k_2, k_3. מהי סיבוכיות ההתקפה שתיארתם?

שאלה 3

בשאלה זו נדון במערכת האותנטיקציה NMAC הבאה (שתוארה בהרצאות). המערכת משתמשת בפונקציית דחיסה $f:\{0,1\}^{n+t} \to \{0,1\}^n$ המתוארת בציור הבא:



נניח כי לכל $k \in \{0,1\}^n$ הפונקציה $f(M,k)$, כפונקציה של M, היא פונקציה חד-חד ערכית ועל. הודעה מורכבת ממספר כלשהו של בלוקים, כל אחד באורך t בדיוק. לחשב אותנטיקציה של הודעה המורכבת מ- ℓ בלוקים, כל אחד עם t ביטים, משתמשים ב- $\ell + 1$ פונקציות דחיסה ובמפתח $\langle k_1, k_2 \rangle$ עם $2n$ ביטים, עפ"י המתואר בציור הבא:



כלומר נגדיר $y_0 \leftarrow k_2$ ו- $y_i = f(M_i, y_{i-1})$ והפלט הוא: $\text{NMAC}\big((M_1,\ldots,M_\ell),(k_1,k_2)\big) = f(y_\ell, k_1)$.
בשאלה זו נראה מדוע n צריך להיות גדול.

סעיף א

עבור NMAC עם מפתח $\langle k_1, k_2 \rangle$ ו- ℓ=2 , זוג הודעות $\langle M_1, M_2 \rangle$ ו- $\langle M'_1, M'_2 \rangle$ מתנגשות אם

$$\text{NMAC}(\langle M_1, M_2 \rangle, \langle k_1, k_2 \rangle) = \text{NMAC}(\langle M'_1, M'_2 \rangle, \langle k_1, k_2 \rangle) .$$

הוכיחו כי אם $\langle M_1, M_2 \rangle$ ו- $\langle M'_1, M'_2 \rangle$ מתנגשות אזי $f\big(M_2, f(M_1, k_2)\big) = f\big(M'_2, f(M'_1, k_2)\big)$.

סעיף ב

כמה הודעות עם שני בלוקים יש להגריל מתוך $\{0,1\}^{2n}$ כך שבהסתברות לפחות 3/4 נקבל התנגשות?

סעיף ג

הוכיחו כי אם $f\big(M_2, f(M_1, k_2)\big) = f\big(M'_2, f(M'_1, k_2)\big)$. אזי לכל M_3 מתקיים

$$\text{NMAC}(\langle M_1, M_2, M_3 \rangle, \langle k_1, k_2 \rangle) = \text{NMAC}(\langle M'_1, M'_2, M_3 \rangle, \langle k_1, k_2 \rangle) .$$

סעיף ד

נסמן ב- S את המספר שחישבתם בסעיף ב. הראו איך אפשר לשבור את NMAC ע"י $O(S)$ הודעות, כלומר השובר יכול לבקש אותנטיקציה של $O(S)$ מסמכים כרצונו ואח"כ למצוא בהסתברות 3/4 הודעה ואותנטיקציה חוקית שלה (כאשר ההודעה אינה אחת מההודעות שעליהם קיבל אותנטיקציה).

שאלה 4

נשתמש ב DES כדי לבנות פונקציית hash עם גודל תחום קבוע. נגדיר $h:\{0,1\}^{112} \to \{0,1\}^{64}$ ע"י:

$$h(x_1, x_2) = \mathrm{DES}(\mathrm{DES}(0^{64}, x_1), x_2)$$

כאשר $|x_1| = |x_2| = 56$.

סעיף א

הראו אלגוריתם שרץ בזמן (בערך) 2^{56} שמקבל ערך y ומוצא x_1, x_2 כך ש $h(x_1, x_2) = y$, או מכריז כי אין x_1, x_2 כנ"ל.

סעיף ב

הראו אלגוריתם אקראי שרץ בזמן (בערך) 2^{32} ומוצא התנגשות בהסתברות גבוהה.