23.11.2014

קריפטוגרפיה: תרגיל 2

הגשה: יום א' 7.12.14 לתא 78 בקומה 1 בניין 37 (שימו לב שרשום על התא "אורי שטמר"). ההגשה בזוגות או ביחידים.

שאלה 1

סעיף א

עבור מחרוזת בינארית A, נסמן ב- $\bar{A}$ את המחרוזת המשלימה (כלומר, המחרוזת בה כל אפס מוחלף באחד ולהפך). הוכיחו כי $\mathrm{DES}(\overline{m},\overline{k}) = \overline{\mathrm{DES}(m,k)}$. 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 2

סעיף א

בסעיף זו תראו איך לשבור גרסה של מערכת הצפנה דמוית AES עם סיבוב אחד. ליתר דיוק, נעסוק במערכת הקריפטוגרפית הבאה.

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:

state

הראו איך במערכת זאת בהינתן הודעה m כלשהי והצפנה שלה c, ניתן בצורה יעילה לחשב את המפתח k_1.

סעיף ב

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

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

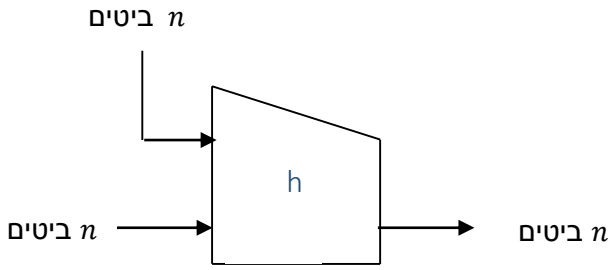
נאמר כי ביט של מפתח משפיע על ביט פלט אם שינוי של הביט במפתח ללא שינוי ביטים אחרים במפתח או בהודעה יכול לשנות את ביט הפלט. נסתכל על ביט כלשהו בפלט של Simple AES. כמה ביטים של המפתח משפיעים על הביט הזה לכל היותר?

סעיף ג

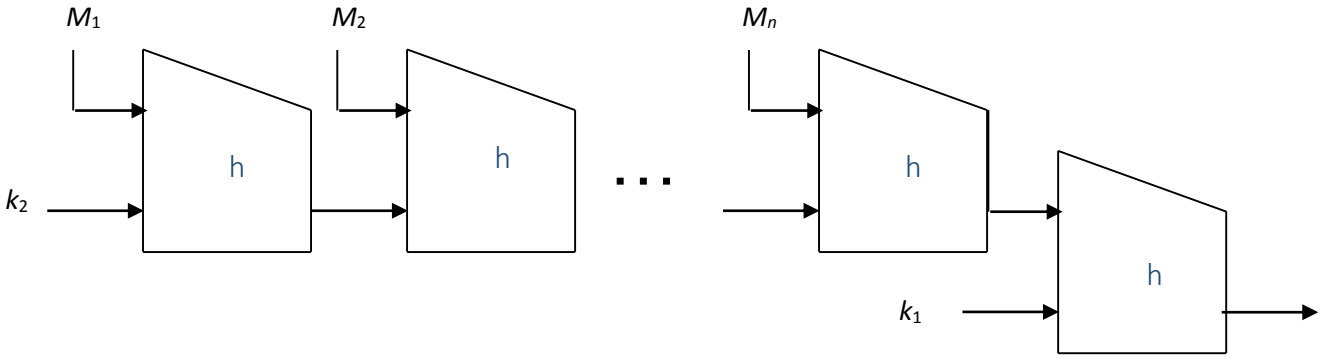
הניחו כי בהינתן זוג קלטים in ו- in' ופלטים out ו- out' קיימת לכל היותר שלשת מפתחות k_1, k_2, k_3 אחת המעתיקה את הקלטים הנ"ל לפלטים המתאימים. תארו התקפה יעילה ככל האפשר המקבלת קלטים in ו- in' ואת הפלטים המתאימים להם out ו- out' ומוצאת את המפתחות k_1, k_2, k_3. מהי סיבוכיות ההתקפה שתיארתם?

שאלה 3

בשאלה זו נדון במערכת האותנטיקציה NMAC הבאה. המערכת משתמשת בפונקציית דחיסה $h:\{0,1\}^{2n} \to \{0,1\}^n$ המתוארת בציור הבא:



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



כלומר נגדיר $y_0 = k_2$ ו- $y_1 \leftarrow h(m_i, y_{i-1})$ והפלט הוא:

$$\mathrm{NMAC}\big((m_1,\dots,m_B),(k_1,k_2)\big) = h(y_n,k_1)$$

שימו לב כי לא משרשרים את אורך ההודעה בבלוק האחרון. בשאלה זו נראה מדוע n צריך להיות גדול.

סעיף א

עבור NMAC עם מפתח (k_1,k_2) ו- B=2 , זוג הודעות (m_1,m_2) ו- (m_1',m_2') מתנגשות אם

$$\mathrm{NMAC}((m_1,m_2),(k_1,k_2)) = \mathrm{NMAC}((m_1',m_2'),(k_1,k_2))$$

הוכיחו כי אם (m_1,m_2) ו- (m_1',m_2') מתנגשות אזי $h\big(m_2,h(m_1,k_2)\big) = h\big(m_2',h(m_1',k_2)\big)$.

סעיף ב

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

סעיף ג

הוכיחו כי אם $h\big(m_2,h(m_1,k_2)\big) = h\big(m_2',h(m_1',k_2)\big)$ אזי לכל m_3 מתקיים

$$\mathrm{NMAC}\big((m_1,m_2,m_3),(k_1,k_2)\big) = \mathrm{NMAC}\big((m_1',m_2',m_3),(k_1,k_2)\big)$$

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

בשאלה זו ניתן להניח כי קיימות פונקציות hash חסינות ממציאת התנגשויות. הוכח או הפרך:

(א) קיימת פונקציית hash חסינה ממציאת התנגשויות כל שלכל t, n מתקיים $h(0^t, 1^n) = 0^n$.

(ב) אם h היא פונקציית hash חסינה ממציאת התנגשויות, אז גם
$$h'(x, 1^n) = h(h(x, 1^n), 1^n)$$

(ג) אם h היא פונקציית hash חסינת התנגשויות, אז גם
$$h'(x \circ y, 1^n) = h(x, 1^n) \oplus h(y, 1^n)$$

(ד) אם h היא פונקציית hash חסינת התנגשויות, אז גם
$$h'(x \circ y, 1^{2n}) = h(x, 1^n) \circ h(y, 1^n)$$

הערה: הסימן $\circ$ פירושו שרשור.
רמז: בדיוק 2 מהטענות הנ"ל נכונות.