קריפטוגרפיה - מועד א'

202-1-5351
סמסטר א' תש"ע
15.1.2010

הנחיות:

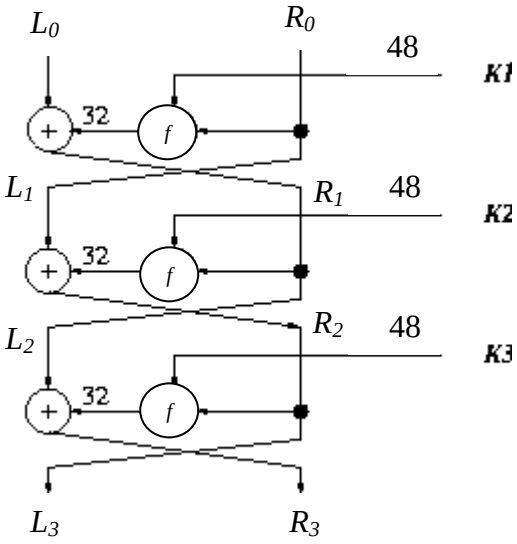
1. בטופס הבחינה 3 דפים מלבד דף זה. ודאו כי כולם נמצאים בידכם.
2. בבחינה 3 שאלות שמשקלן אינו שווה. יש לענות על כולן.
3. הבחינה עם חומר פתוח.
4. נמקו את כל תשובותיכם. פתרון ללא הוכחה לא יתקבל.
5. משך הבחינה 3 שעות.
6. מומלץ לא להתעכב זמן רב מדי על שום סעיף.
7. הנכם רשאים להסתמך על סעיפים קודמים, גם אם לא השבתם עליהם.
8. מותר להסתמך על משפטים שהוכחו בהרצאות, אך יש לצטט אותם במדויק.
9. אם אתם מסתמכים על טענות שהוכחו בתרגילי בית יש להוכיח אותם.

01. במידה ואינכם יודעים את התשובה לסעיף כלשהו, רשמו "לא יודעים" ותזכו ב- 20% מניקוד הסעיף.

בהצלחה!

שאלה 1 [30 נקודות]

בשאלה זו נראה איך לשבור מערכת הצפנה דמוית DES עם 3 סיבובים כאשר משתמשים בשלושה מפתחות בלתי תלויים בני 48 ביטים כל אחד. ליתר דיוק, נעסוק במערכת הקריפטוגרפית המצוירת לעיל.



במערכת זאת, אם ניקח שלושה זוגות הודעות וקריפטוגרמות $\langle M_1,C_1\rangle,\langle M_2,C_2\rangle,\langle M_3,C_3\rangle$ אזי בהסתברות גבוהה יהיה לכל היותר מפתח $k=\langle k_1,k_2,k_3\rangle$ יחיד שיעתיק כל M_i ל- C_i.

סעיף א [8 נקודות]

הראו התקפת הודעה נתונה על המערכת בסיבוכיות זמן סדר גודל של $2^{3\cdot 48}$ ובזיכרון $O(1)$.

סעיף ב [7 נקודות]

הראו איך לבטא את L_2,R_2 כפונקציה של L_3,R_3 ו- K_3.

סעיף ג [15 נקודות]

הראו התקפת הודעה נתונה על המערכת בסיבוכיות זמן סדר גודל של $2^{2\cdot 48}$ ובזיכרון 2^{48}.

שאלה 2 [25 נקודות]

סעיף א [10 נקודות]

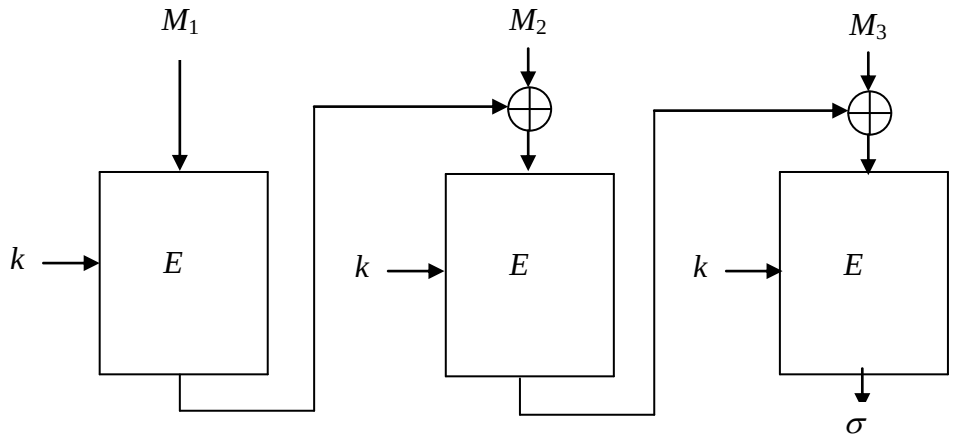
במערכת ההצפנה של Blum-Goldwasser, שאותה לא נתאר, אלגוריתם יצירת המפתחות מגריל שני ראשוניים גדולים p,q, מחשב $N=p\cdot q$ ושני מספרים a,b כך ש- $ap+bq=1$. המפתח הפרטי הוא N,a,b והמפתח הציבורי הוא N. הוכיחו כי אם ידוע המפתח הפרטי אזי ניתן באופן יעיל לחשב את p,q.

סעיף ב [15 נקודות]

לשני משתמשים יש מפתחות ציבוריים של מערכת ההצפנה RSA עם אותו N, כלומר המפתחות הציבוריים שלהם הם $\langle N,e_1\rangle$ ו- $\langle N,e_2\rangle$. כמו כן נתון כי $e_1\neq e_2$ ו- $\gcd(e_1,e_2)=1$. אותה הודעה הוצפנה ע"י שני המפתחות. הראו כי מתקיף המחזיק ב- $N,e_1,e_2,m^{e_1}\bmod N,m^{e_2}\bmod N$ יכול לשחזר את m בצורה יעילה.

שאלה 3 [45 נקודות]

בשאלה זו נדון במערכת האותנטיקציה CBC-MAC הבאה (שתוארה בהרצאות). המערכת משתמשת בפונקציית הצפנה $E:\{0,1\}^n\times\{0,1\}^k\to\{0,1\}^n$, כלומר אורך ההודעה והקריפטוגרמה הוא n ואורך המפתח הוא k, ולמערכת קיימת פונקציית פענוח. נשתמש במערכת זאת לבצע אותנטיקציה של הודעות המכילות בדיוק שלושה בלוקים, כל אחד עם n ביטים. המערכת מתוארת בציור הבא, כאשר σ הוא הפלט.



בשאלה זו נראה התקפה על המערכת המבוססת על פרדוקס יום ההולדת.

סעיף א [10 נקודות]

הוכיחו כי לכל k אם נגריל M_1,M_2,M_3 בהתפלגות אחידה אזי σ יתפלג בהתפלגות אחידה ב- $\{0,1\}^n$.

עבור CBC-MAC עם מפתח k נאמר כי שתי הודעות $\langle M_1,M_2\rangle$ ו- $\langle M'_1,M'_2\rangle$, עם שני בלוקים כל אחת, מתנגשות אם

1. $E(E(M_1,k)\oplus M_2,k)=E(E(M'_1,k)\oplus M'_2,k)$.
2. $\langle M_1,M_2\rangle\neq\langle M'_1,M'_2\rangle$.

סעיף ב [10 נקודות]

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

סעיף ג [10 נקודות]

הוכיחו כי האלגוריתם הבא מוצא זוג הודעות מתנגשות בהסתברות גבוהה.

1. $i\leftarrow 1$
2. הגרל M_1^i,M_2^i ובקש אותנטיקציה $\sigma_i\leftarrow\text{CBC-MAC}(\langle M_1^i,M_2^i,0^n\rangle,k)$
3. אם $\sigma_i=\sigma_j$ עבור $j<i$ עצור, אחרת $i\leftarrow i+1$ ולך ל 2.

סעיף ד [15 נקודות]

נסמן ב- S את המספר שחישבתם בסעיף ב. הראו איך אפשר לשבור את CBC-MAC ע"י $S+O(1)$ הודעות, כלומר השובר יכול לבקש אותנטיקציה של $S+O(1)$ הודעות כרצונו (כל הודעה עם שלושה בלוקים) ואח"כ למצוא בהסתברות 3/4 הודעה עם שלושה בלוקים ואותנטיקציה חוקית שלה (כאשר ההודעה אינה אח ת מההודעות שעליהם קיבל אותנטיקציה).