עמוס ביימל
ענב וינרב

המחלקה למדעי המחשב

קריפטוגרפיה - מועד א'

202-1-5351

סמסטר ב' תשס"ד

7.7.2004

הנחיות:

1. בטופס הבחינה שני דפים מלבד דף זה. ודאו כי כולם נמצאים בידכם.
2. בבחינה 4 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 להיתקע 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 במדוייק.
9. אם אתם מסתמכים על טענות שהוכחו בתרגילי בית יש להוכיח אותם.

בהצלחה!

שאלה 1 [35 נקודות]

יהיו p , q ו-r מספרים ראשוניים גדולים מ-2 ושונים זה מזה ו- $N=pqr$.
בשאלה זו נעסוק במערכת חתימה המבוססת על מערכת החתימה של רבין.
מפתח חתימה פרטי: $<p, r, q>$.
מפתח וידוא ציבורי: N.
חתימה על הודעה $m \in \mathbb{Z}_N^*$: החותם מחשב $a \in \mathbb{Z}_N^*$, כך שיתקיים $m \equiv a^2 \bmod N$.
וידוא חתימה $a \in \mathbb{Z}_N^*$ על הודעה $m \in \mathbb{Z}_N^*$: המוודא בודק כי $m \equiv a^2 \bmod N$.

סעיף א [5 נקודות]

הוכיחו כי אם $m \in \mathbb{Z}_N^*$ הוא ריבוע מודולו N אזי המספר $m \bmod p$ הוא ריבוע מודולו p, המספר $m \bmod q$ הוא ריבוע מודולו q, והמספר $m \bmod r$ הוא ריבוע מודולו r.

סעיף ב [8 נקודות]

יהי $m \in \mathbb{Z}_N^*$ כך שהמספר $m \bmod p$ הוא ריבוע מודולו p, המספר $m \bmod q$ הוא ריבוע מודולו q, והמספר $m \bmod r$ הוא ריבוע מודולו r. הוכיחו כי m הוא ריבוע מודולו N.

סעיף ג [8 נקודות]

נתון $a \equiv c^2 \bmod N$, עבור $a, c \in \mathbb{Z}_N^*$.
הראו כי בהינתן p, q ו-r, ניתן למצוא בצורה יעילה 8 שורשים שונים של a מודולו N (כולל c).

סעיף ד [7 נקודות]

הראו כי על ידי התקפת הודעה נבחרת ניתן, בהסתברות גבוהה, למצוא בצורה יעילה גורם לא טריוויאלי כלשהו של N.

סעיף ה [7 נקודות]

הראו כי על ידי התקפת הודעה נבחרת ניתן, בהסתברות גבוהה, לפרק את N לשלושת גורמיו הראשוניים.

שאלה 2 [15 נקודות]

נתונים $M, C \in \{0,1\}^{64}$ ו-$K \in \{0,1\}^{56}$, כך ש- $\mathrm{DES}(M, K) = C$.

סעיף א [2 נקודות]

הראו כי אם איב יודעת את M ו-K היא יכולה לחשב את L_8, R_8 (תוצאת הביניים ה-8 בחישוב DES).

סעיף ב [5 נקודות]

הראו כי אם איב יודעת את C ו-K היא יכולה לחשב את L_8, R_8.

סעיף ג [8 נקודות]

נקודת שבת של DES עם מפתח 0^{56} היא הודעה M כך ש- $M = \mathrm{DES}(M, 0^{56})$. הוכיחו כי יש <u>לכל היותר</u> 2^{32} נקודות שבת.
תזכורת: בתרגיל בית הוכחנו כי יש לפחות 2^{32} נקודות שבת.

שאלה 3 [30 נקודות]

יהי p ראשוני, ויהי g יוצר של $\mathbb{Z}_p^*$. שלשת DH היא שלשה $\langle A,B,C\rangle \in \left(\mathbb{Z}_p^*\right)^3$ אם קיימים $a,b \in \mathbb{Z}_{p-1}$ כך ש- $A \equiv g^a \pmod p$, $B \equiv g^b \pmod p$ ו- $C \equiv g^{ab} \pmod p$.

<u>הנחת ההכרעה של Diffie ו-Hellman (להלן הנחת DDH):</u>

לא קיים אלגוריתם יעיל שבהינתן $\langle A,B,C\rangle \in \left(\mathbb{Z}_p^*\right)^3$ מכריע האם הקלט הוא שלשת DH.

בשאלה זו נבנה פרוטוקול Private Information Retrieval (PIR) תחת הנחת ההכרעה של Diffie ו-Hellman.

סעיף א [6 נקודות]

נתונות שתי שלשות DH הבאות: $\langle A,B_1,C_1\rangle$ **ו-** $\langle A,B_2,C_2\rangle$**.** הראו כי $\langle A,B_1B_2,C_1C_2\rangle$ היא שלשת DH.

סעיף ב [7 נקודות]

נתונה שלשת DH $\langle A,B_1,C_1\rangle$. מאידך, ידוע כי $\langle A,B_2,C_2\rangle$ אינה שלשת DH. הוכיחו כי $\langle A,B_1B_2,C_1C_2\rangle$ אינה שלשת DH.

סעיף ג [7 נקודות]

אליס מחזיקה $B,C \in \mathbb{Z}_p^*$ ו- $a \in \mathbb{Z}_{p-1}$. תארו כיצד אליס יכולה לחשב בצורה יעילה האם $\langle g^a,B,C\rangle$ היא שלשת DH.

סעיף ד [10 נקודות]

תכננו פרוטוקול PIR בעל סיבוכיות תקשורת $O(n)$ מהמשתמש לשרת, וסיבוכיות תקשורת $O(1)$ מהשרת למשתמש הבטוח אם הנחת DDH נכונה. הוכיחו את בטיחות הפרוטוקול.

הדרכה: תכננו פרוטוקול הדומה לפרוטוקול PIR (שתואר בכיתה) על סמך הנחת השאריות הריבועיות.

שאלה 4 [20 נקודות]

תהי $h:\{0,1\}^{b+1} \to \{0,1\}^b$ פונקציה קלה לחישוב.

הפונקציה h היא *פונקצית דחיסה* אם בהינתן $x \in \{0,1\}^{b+1}$ קשה למצוא $x' \in \{0,1\}^{b+1}$ כך ש- $x' \neq x$ ו- $h(x)=h(x')$.

הפונקציה h היא *פונקציה חד-כיוונית* אם בהינתן $y \in \{0,1\}^b$ קשה למצוא $x \in \{0,1\}^{b+1}$ כך ש- $h(x)=y$.

סעיף א [8 נקודות]

נאמר כי $x \in \{0,1\}^{b+1}$ הוא *בודד* אם לא קיים $x' \in \{0,1\}^{b+1}$ כך ש- $x' \neq x$ ו- $h(x)=h(x')$. הוכיחו כי קיימים לפחות 2^b+1 x-ים שאינם בודדים.

סעיף ב [12 נקודות]

הוכיחו כי אם h היא פונקצית דחיסה אזי היא חד-כיוונית.

<u>הדרכה</u>: h היא אינה פונקציית דחיסה אם בהסתברות גדולה מ- $\frac{1}{4}$ ניתן למצוא x' כנ"ל.