עמוס ביימל
ענב וינרב

המחלקה למדעי המחשב

אוניברסיטת בן-גוריון בנגב
Ben-Gurion University of the Negev

קריפטוגרפיה - מועד ב'

202-1-5351
סמסטר ב' תשס"ד
28.7.2004

הנחיות:

1. בטופס הבחינה שלושה 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 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 במדויק.
9. אם אתם מסתמכים על טענות שהוכחו בתרגילי בית יש להוכיח אותם.
10. ניתן לענות על סעיף "לא יודעים". במקרה זה תקבלו 20% מניקוד הסעיף.

בהצלחה!

שאלה 1 [32 נקודות]

שאלה זאת עוסקת במערכת ההצפנה DES.

סעיף א [8 נקודות]

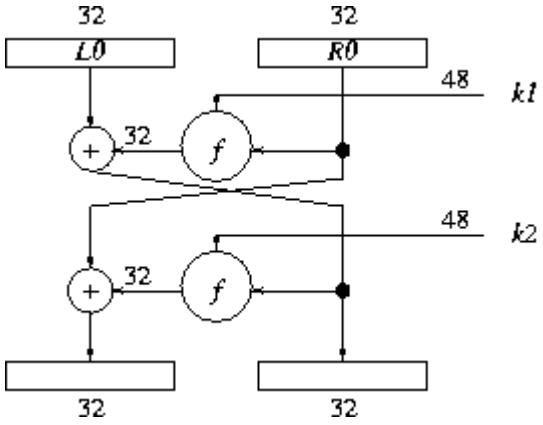
נסתכל על S-box כלשהי S_i, באשר $1 \le i \le 8$. הסבירו מדוע לכל פלט אפשרי $y \in \{0,1\}^4$ של S_i קיימים בדיוק 4 קלטים $x \in \{0,1\}^6$ ל- S_i עבורם מתקיים $S_i(x) = y$.

סעיף ב [12 נקודות]

נסתכל על פונקציית f של DES. נקבע הודעה שרירותית $M \in \{0,1\}^{64}$ ונסמן $M = L_0 R_0$, באשר $L_0, R_0 \in \{0,1\}^{32}$.
הוכיחו כי לכל פלט אפשרי $y \in \{0,1\}^{32}$ של $f(R_0, k_1)$ קיימות בדיוק 2^{16} אפשרויות לבחירת $k_1 \in \{0,1\}^{48}$ עבורן מתקיים $f(R_0, k_1) = y$.

סעיף ג [12 נקודות]

נסתכל על גרסת DES בת שני סיבובים, עם שני מפתחות בלתי תלויים $k_1, k_2 \in \{0,1\}^{48}$, כמתואר באיור הבא:



הוכיחו כי לכל הודעה $M \in \{0,1\}^{64}$ וקריפטוגרמה $C \in \{0,1\}^{64}$ קיימים בדיוק 2^{32} זוגות של מפתחות $k_1, k_2 \in \{0,1\}^{48}$ עבורם מתקיים $\mathrm{DES}(M, \langle k_1, k_2 \rangle) = C$.

שאלה 2 [33 נקודות]

שאלה זו עוסקת בסכמות לחלוקת סוד. נגדיר מבנה גישה על $n = n_1 n_2$ משתתפים המחולקים ל-n_1 קבוצות זרות בגודל n_2 כל קבוצה. נתונים $t_1 \le n_1$ ו-$t_2 \le n_2$, ונגדיר כי קבוצה S מתקבלת אם ישנן לפחות t_1 קבוצות כך ש-S מכילה לפחות t_2 משתתפים שלהן.

סעיף א [3 נקודות]

הוכיחו כי מבנה סף הוא מקרה פרטי של מבנה הגישה המתואר בשאלה.

סעיף ב [30 נקודות]

1. [12 נקודות] בנו סכימה לחלוקת סוד עבור מבנה הגישה המתואר כאשר הסוד והחלקים הניתנים לשחקנים לקוחים מתוך $\mathbb{Z}_p$ עבור $p > n$.
2. [9 נקודות] הוכיחו כי כל קבוצה השייכת למבנה הגישה אכן יכולה לשחזר את הסוד.
3. [9 נקודות] הראו כי לכל קביעה של חלקי סוד לקבוצה לא משחזרת T, כל סוד $s \in \mathbb{Z}_p$ הוא אפשרי (כלומר, לכל $s \in \mathbb{Z}_p$ קיימת חלוקה של הסוד s בה החלקים הניתנים לשחקני T הם אותם החלקים בדיוק.)

שאלה 3 [35 נקודות]

שאלה זו עוסקת בפרוטוקול Oblivious Transfer המתבסס על הנחת ההכרעה של Diffie ו-Hellman.

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.

שלוש העובדות הבאות הוכחו במועד א' <u>ואין צורך להוכיחן</u> במועד זה:

1. בהינתן שתי שלשות DH $\langle A,B_1,C_1\rangle$ ו- $\langle A,B_2,C_2\rangle$, גם השלשה $\langle A,B_1B_2,C_1C_2\rangle$ היא שלשת DH.
2. אם $\langle A,B_1,C_1\rangle$ היא שלשת DH, ומאידך, $\langle A,B_2,C_2\rangle$ אינה שלשת DH, אזי השלשה $\langle A,B_1B_2,C_1C_2\rangle$ אינה שלשת DH.
3. בהינתן $B,C \in \mathbb{Z}_p^*$ ו- $a \in \mathbb{Z}_{p-1}$, השלשה $\langle g^a,B,C\rangle$ היא שלשת DH אם ורק אם $B^a \equiv C \pmod p$.

נזכיר את הגדרת פרוטוקול Oblivious Transfer:

קלט לאליס: $i \in \{0,1\}$.

קלט לבוב: $y_0,y_1 \in \{0,1\}$.

דרישות:

נכונות: בסיום הפרוטוקול אליס תדע את y_i.

בטיחות 1: אליס לא תלמד דבר על y_{1-i}.

בטיחות 2: בוב לא ילמד דבר על i.

הוצע הפרוטוקול הבא עבור Oblivious Transfer:

1. אליס מגרילה $a,b_{1-i} \in \mathbb{Z}_{p-1}$, ומחשבת את השלשה $\langle A,B_{1-i},C_{1-i}\rangle$ כאשר $A=g^a$, $B_{1-i}=g^{b_{1-i}}$ ו- $C_{1-i}=g^{ab_{1-i}}$.
2. אליס מגרילה $x,b_i \in \mathbb{Z}_{p-1}$, ומחשבת את השלשה $\langle A,B_i,C_i\rangle$ כאשר $A=g^a$, $B_i=g^{b_i}$ ו- $C_i=g^x$, באשר $x \not\equiv ab_i \pmod{p-1}$.
3. אליס שולחת את השלשות $\langle A,B_0,C_0\rangle$ ו- $\langle A,B_1,C_1\rangle$ לבוב.
4. בוב מחשב $B=B_0^{y_0}B_1^{y_1} \bmod p$ ו- $C=C_0^{y_0}C_1^{y_1} \bmod p$.
5. בוב שולח את $\langle B,C\rangle$ לאליס.
6. אליס בודקת האם $\langle A,B,C\rangle$ היא שלשת DH. אם כן, היא קובעת $y_i=0$. אחרת, היא קובעת $y_i=1$.

סעיף א [5 נקודות]

הוכיחו את נכונות הפרוטוקול, כלומר, שהביט שאליס מחשבת הוא אכן y_i.

סעיף ב [5 נקודות]

הסבירו מדוע בוב לא לומד מידע על i.

סעיף ג [10 נקודות]

הפרוטוקול הנ"ל אינו עונה על דרישת בטיחות 1. הראו כיצד אליס יכולה לחשב בצורה יעילה את y_0 ו- y_1.

סעיף ד [5 נקודות]

הוכיחו כי לכל $r \in \mathbb{Z}_{p-1}$, השלשה $\langle A, g^r, A^r \rangle$ היא שלשת DH.

סעיף ה [10 נקודות]

להלן הצעה לתיקון הפרוטוקול הבתון:
נחליף את שלב 5 בפרוטוקול בשלבים:

5. א. בוב מגריל $r \in \mathbb{Z}_{p-1}$ ומחשב $B \leftarrow Bg^r$ ו- $C \leftarrow CA^r$.

ב. בוב שולח את $\langle B, C \rangle$ לאליס.

הוכיחו כי הפרוטוקול החדש עונה לכל דרישות Oblivious Transfer.