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

קריפטוגרפיה - מועד ב'

202-1-5351
סמסטר א' תשס"ח
13.7.2008

הנחיות:

1. בטופס הבחינה 4 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.
10. **במידה ואינכם יודעים את התשובה לסעיף כלשהו, רשמו "לא יודעים" ותזכו ב- 20% מניקוד הסעיף.**

בהצלחה!

שאלה 1 [35 נקודות]

נתון כי p הוא ראשוני אי-זוגי ו- $q=2p+1$. נתאר אלגוריתם לבדיקה אם q ראשוני.

1. הגרל a באקראי מהקבוצה $\{2,...,q-2\}$.
2. אם $\gcd(a,q)\neq 1$ הכרז "q אינו ראשוני" וסיים.
3. אם
   a. $a^{2p}\equiv 1 (\mathrm{mod}\, q)$ ו-
   b. $a^{p}\not\equiv 1 (\mathrm{mod}\, q)$ ו-
   c. $a^{2}\not\equiv 1 (\mathrm{mod}\, q)$

   הכרז "q ראשוני", אחרת הכרז "q אינו ראשוני".

מטרת הסעיפים הבאים היא להוכיח את נכונות האלגוריתם.

סעיף א [3 נקודות]

יהי $q=7$. מהם ערכי a עבורם האלגוריתם יחזיר כי q ראשוני?

סעיף ב [7 נקודות]

הוכיחו כי עבור כל $q=2p+1$ ראשוני, האלגוריתם יחזיר כי q ראשוני בהסתברות לפחות 0.5.

סעיף ג [8 נקודות]

יהי $a\in \mathbf{Z}_q^*$ כך ש- $a^{2p}\equiv 1 (\mathrm{mod}\, q)$. נסמן ב- i את הסדר של a ב- $\mathbf{Z}_q^*$. הוכיחו כי i מחלק את $2p$ ואת $\varphi(q)$.

סעיף ד [11 נקודות]

הוכיחו כי אם $q=2p+1$ אינו ראשוני אזי לכל a האלגוריתם יכריז כי "q אינו ראשוני".

סעיף ה [6 נקודות]

מהי סיבוכיות האלגוריתם?

שאלה 2 [30 נקודות]

נסתכל על הרעיון הבא לסכמה לחלוקת סוד 3-מתוך-n. יהי $p>n$ ראשוני.

קלט: סוד $s \in \mathbf{Z}_p$

- הגרל שני איברים $r_2, r_0 \in \mathbf{Z}_p$ בהתפלגות אחידה ובאופן בלתי תלוי.
- הגדר את הפולינום $Q(x) = r_2 x^2 + sx + r_0$.
- החלק של משתמש i (כאשר $1 \le i \le n$) הוא $s_i = Q(i) \bmod p$.

סעיף א [5 נקודות]

הראו כי כל קבוצה בגודל 3 יכולה לשחזר את הסוד.

סעיף ב [10 נקודות]

הראו כי זוג המשתתפים i ו- p-i יכולים לשחזר את הסוד. הסיקו כי הסכמה אינה סכמה לחלוקת סוד 3-מתוך-n.

סעיף ג [7 נקודות]

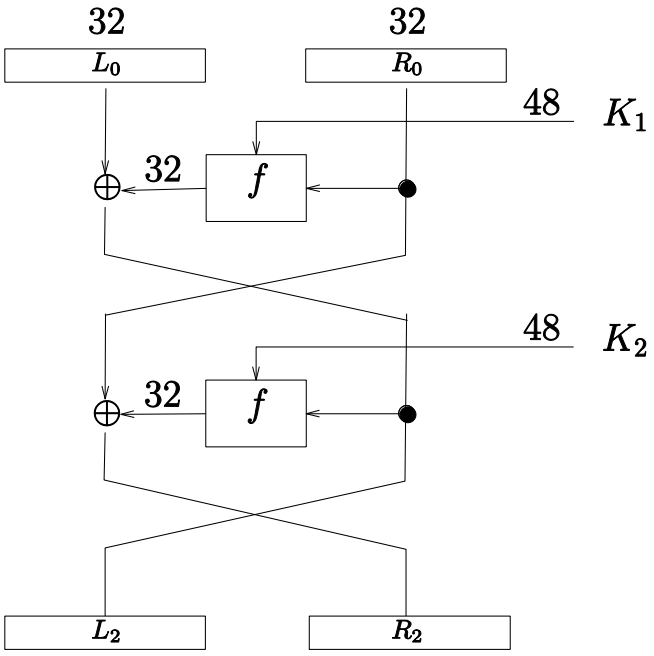
יהיו $i, j \in \mathbf{Z}_p$ כך ש- $i^2 \not\equiv j^2 \pmod p$. הוכיחו כי לכל $\alpha, \beta \in \mathbf{Z}_p$ קיים פולינום $R(x)$ מעל $\mathbf{Z}_p$ שדרגתו 2, המקדם של x הוא אפס, $R(i) = \alpha$ ו- $R(j) = \beta$.

סעיף ד [8 נקודות]

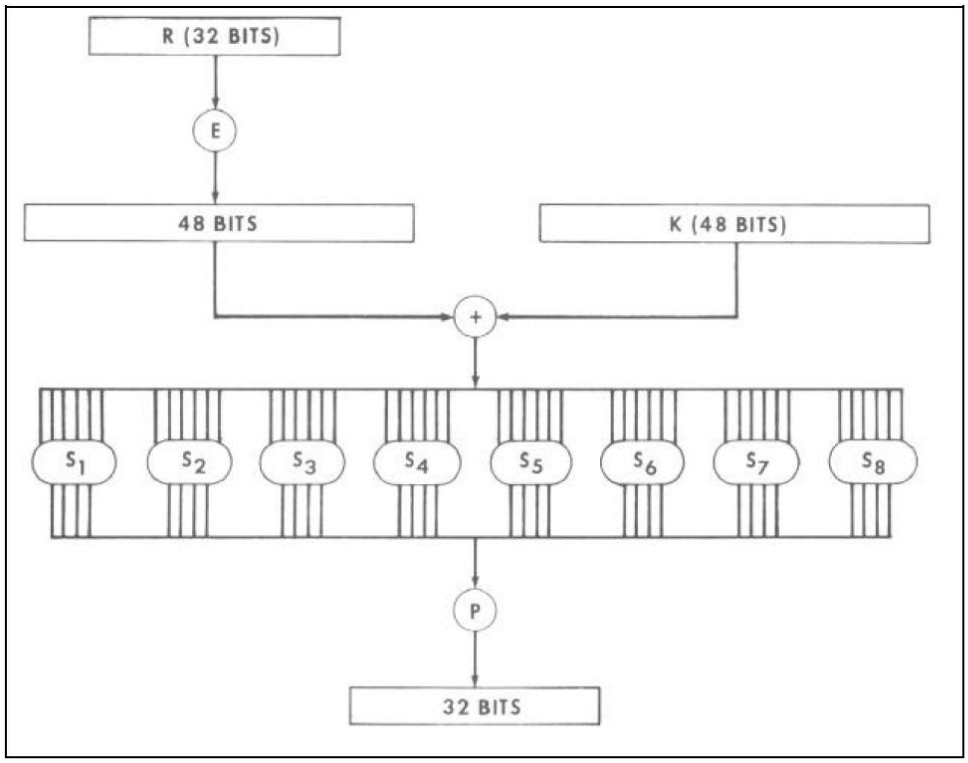
נשנה את הסכמה כך שכעת $p>2n$. הוכיחו כי בסכמה החדשה כל קבוצה בגודל 2 לא לומדת מידע על הסוד.

שאלה 3 [25 נקודות]

בפונקצית f במערכת ההצפנה DES ישנה פונקציה P "המערבבת" את סדר הביטים היוצאים מקופסאות ה-S. בשאלה זו נדגים את חשיבות פונקציה זו. נסתכל על גרסת DES בת שני סיבובים המוארת באיור הבא. במערכת יש שני מפתחות בלתי תלויים $k_1, k_2 \in \{0,1\}^{48}$, הקלט הוא L_0, R_0 והפלט הוא L_2, R_2.



הפונקציה f מתוארת באיור הבא, כאשר P היא פונקצית הזהות.



הפונקציה E מתוארת בטבלה הבאה.

E BIT-SELECTION TABLE

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

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.

סעיף א [5 נקודות]

נסתכל על ביט כלשהו בפלט של f . הראו כי לכל היותר 6 ביטים של המפתח משפיעים על הביט.

סעיף ב [10 נקודות]

נסתכל על ביט כלשהו ב- R_2. הראו כי לכל היותר 24 ביטים של המפתח משפיעים על הביט.

סעיף ג [10 נקודות]
נשתמש כעת בפונקציה P המקורית של DES המתוארת בטבלה הבאה:

16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

נסתכל על ביט כלשהו ב- R_2. הסבירו מדוע ב- DES עם P המקורית כל ביט של k_1 ישפיע על הביט.
הערה: מותר להניח כי לכל ביט בקלט של קופסת S וכל ביט בפלט שלה, ביט הקלט משפיע על ביט הפלט, כלומר קיימת הצבה לביטי הקלט האחרים של קופסת ה- S כך שעבור שתי ההצבות האפשריות לביט הקלט נקבל שני ערכים שונים לביט הפלט.