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

קריפטוגרפיה - מועד א'

202-1-5351
סמסטר א' תשס"ח
2.5.2008

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 [25 נקודות]

תזכורת: שיטת החתימה של RSA (ללא hash) מוגדרת בצורה הבאה:

אלגוריתם יצירת המפתחות:

1. הגרל 2 מספרים ראשוניים גדולים p,q וחשב $N=pq$.
2. הגרל $e\in\mathbf{Z}^*_{\varphi(N)}$ וחשב $d=e^{-1} \bmod \varphi(N)$.

מפתח הוידוא הציבורי: N,e.

מפתח החתימה הפרטי: N,d.

החתימה על הודעה $M\in\mathbf{Z}^*_{N_1}$ כאשר $M>1$ היא $\mathrm{RSA}(M,(N,d))=M^d \bmod N$.

בהרצאה הראינו כי שיטה זו אינה עמידה כנגד שבירה קיומית וכנגד התקפת הודעה נבחרת. כדי להתגבר על בעיות אילו הוצע לקודד קודם את ההודעה ואח"כ לחתום, כלומר לקחת פונקציה encode הידועה לכל המשתתפים והחתימה על הודעה היא $\text{encode-RSA}(M,(N,d))=(\text{encode}(M))^d \bmod N$. בשאלה זו נדון בשיטות לא טובות לבחירה של פונקצית הקידוד.

סעיף א [3 נקודות]

איך מוודאים כי חתימה בשיטת encode-RSA היא חוקית?

סעיף ב [10 נקודות]

נגדיר $\text{encode}_1(M)=4M$ עבור $M<N/4$. הראו התקפה קיומית הרצה בזמן פולינומי על שיטה זו בה המתקיף רואה את המפתח הציבורי ומצליח לייצר בהסתברות גבוהה זוג M,S כך ש- $S\equiv(\text{encode}_1(M))^d \pmod N$ ו- $M<N/4$. הוכיחו כי החתימה שהתקפה מייצרת היא חוקית וזמן הריצה של ההתקפה הוא פולנומי.

סעיף ג [12 נקודות]

נגדיר $\text{encode}_2(M)=2^{n/4}M$ עבור $M<N/2^{n/4}$ כאשר $n=\lfloor \log N \rfloor$. הראו התקפה קיומית על שיטה זו בה המתקיף רואה את המפתח הציבורי, יכול לבקש חתימות על שני מסמכים כרצונו, ומצליח לייצר זוג M,S כך ש- $M<N/4$ ו- $S\equiv(\text{encode}_2(M))^d \pmod N$. הוכיחו כי החתימה שהתקפה מייצרת היא חוקית וזמן הריצה של ההתקפה הוא פולנומי.

הדרכה: אפשר להיעזר בתכונת הכפליות של ה- RSA.

שאלה 2 [35 נקודות]

נסתכל על מערכת האותנטיקציה הבאה:

- יצירת המפתחות: יהי p ראשוני גדול. המפתח הוא שני איברים $a,b \in \mathbf{Z}_p$ המוגרלים בהתפלגות אחידה ובאופן בלתי תלוי.
- האותנטיקציה של הודעה $x \in \mathbf{Z}_p$ היא $\mathrm{AUTH}(x,(a,b)) = (ax+b) \bmod p$.

סעיף א [12 נקודות]

הראו כי איב היכולה לבקש אותנטיקציה של הודעה אחת $x \in \mathbf{Z}_p$ (אך אינה יודעת מהו המפתח), אינה יכולה לייצר בהסתברות גדולה מ- $1/p$ זוג $y,z \in \mathbf{Z}_p$ כך ש- $y \neq x$ ו- $z = \mathrm{AUTH}(y,(a,b))$.

סעיף ב [10 נקודות]

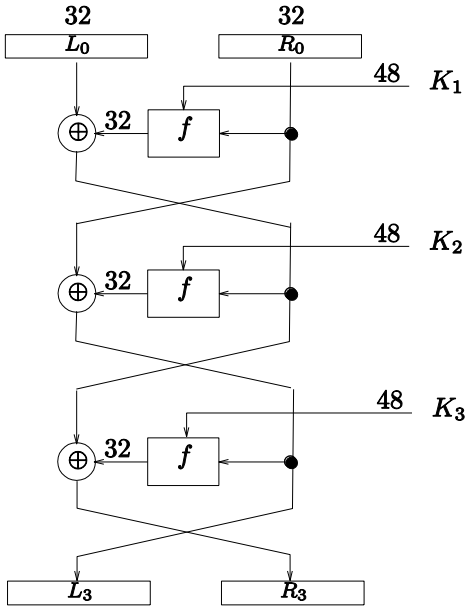
הראו כי איב הרואה אותנטיקציה של שתי הודעות $x,x' \in \mathbf{Z}_p$ כך ש- $x' \neq x$ (אך אינה יודעת מהו המפתח) יכולה לייצר זוג $y,z \in \mathbf{Z}_p$ כך ש- $y \neq x,x'$ ו- $z = \mathrm{AUTH}(y,(a,b))$.

סעיף ג [13 נקודות]

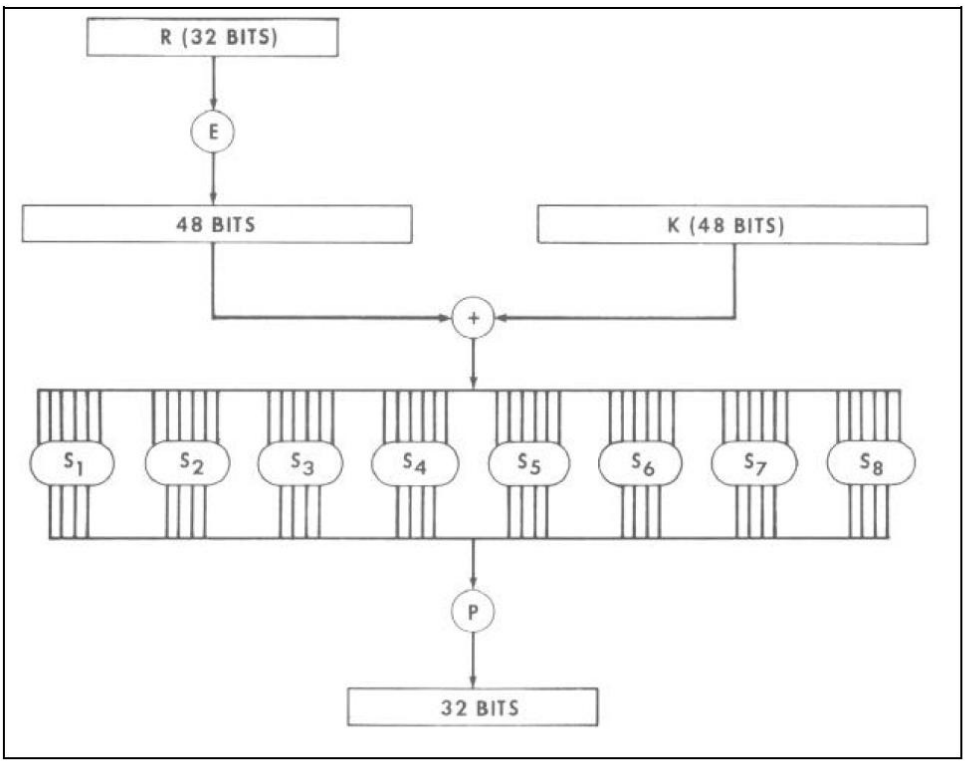
בנו מערכת אותנטיקציה בה איב היכולה לבקש אותנטיקציה של t הודעות (אך אינה יודעת מהו המפתח) אינה יכולה לייצר בהסתברות גדולה מ- $1/p$ זוג $y,z \in \mathbf{Z}_p$ כך ש- y שונה מההודעות שאיב ביקשה ו- $z = \mathrm{AUTH}(y,(a,b))$. הוכיחו בנייתכם.

שאלה 3 [40 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 שלושה סיבובים המוארת באיור הבא. במערכת יש שלושה מפתחות בלתי תלויים $k_1, k_2, k_3 \in \{0,1\}^{48}$, הקלט הוא L_0, R_0 והפלט הוא L_3, R_3.



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

סעיף א [5 נקודות]

הסבירו בקיצור איך מפענחים הודעות במערכת זו כאשר k_1, k_2, k_3 ידועים.

בסעיפים הבאים נראה התקפה על המערכת כאשר k_1, k_2, k_3 אינם ידועים. 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 ב [5 נקודות]

כמה ביטים של המפתח משפיעים על כל ביט בפלט של f?

סעיף ג [10 נקודות]

הראו כי 24 ביטים במפתח משפיעים על כל ביט ב- L_3.

סעיף ד [10 נקודות]

הניחו כי בהינתן זוג קלטים L_0, R_0 ו L_0', R_0' ופלטים L_3, R_3 ו L_3', R_3' קיימת לכל היותר שלישיית מפתחות k_1, k_2, k_3 אחת המעתיקה את הקלטים הנ"ל לפלטים המתאימים.
תארו התקפה יעילה ככל האפשר המקבלת קלטים L_0, R_0 ו L_0', R_0' והפלטים המתאימים להם L_3, R_3 ו L_3', R_3' ומוצאת את המפתחות k_1, k_2.

סעיף ה [10 נקודות]

הסבירו למה ההתקפה שתיארתם בסעיף ד אינה עובדת כאשר P היא הפונקציה שבה משתמשים ב- DES המקורי?