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

קריפטוגרפיה - מועד ב'

202-1-5351
סמסטר ב' תשס"ז
13.8.2007

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 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 [40 נקודות]

יהיו p,q ו- $N=pq$ כך ש- $p<q$. כמו כן, יהיו $0 \le x_1 < x_2 < ... < x_t < p$ ו- $y_1, y_2, ..., y_t \in \mathbf{Z}_N$.

סעיף א [10 נקודות]

הוכיחו כי קיים פולינום Q מעל $\mathbf{Z}_N$ מדרגה לכל היותר t-1 כך ש- $Q(x_i) = y_i$ עבור $1 \le i \le t$.

סעיף ב [5 נקודות]

יהי Q פולינום מעל $\mathbf{Z}_N$ כאשר $Q(x) = \sum_{j=0}^{t-1} a_j x^j$. נגדיר $b_j = a_j \bmod p$ עבור $0 \le j \le t-1$ ו- $R(x) = \sum_{j=0}^{t-1} b_j x^j$.
הסבירו מדוע $Q(z) \equiv R(z) (\bmod p)$ לכל $z \in \mathbf{Z}_p$.

סעיף ג [5 נקודות]

יהיו $0 \le x_1 < x_2 < ... < x_t < p$ ו- $y_1, y_2, ..., y_t \in \mathbf{Z}_N$. הוכיחו כי קיים פולינום יחיד R מעל $\mathbf{Z}_p$ מדרגה לכל היותר $t-1$ כך ש- $R(x_i) \equiv y_i (\bmod p)$ עבור $1 \le i \le t$. איפה השתמשתם בכך ש- $x_t < p$?

סעיף ד [12 נקודות]

הוכיחו בעזרת משפט השאריות הסיני כי קיים פולינום יחיד Q מעל $\mathbf{Z}_N$ מדרגה לכל היותר t-1 כך ש- $Q(x_i) = y_i$ עבור $1 \le i \le t$.

סעיף ה [8 נקודות]

יהיו מעל $\mathbf{n}, t$ שלמים חיוביים כך ש- $\mathbf{1} \le t \le n < p < q$. נממש את הסכמה של שמיר מעל $\mathbf{Z}_N$. כלומר כדי לחלק סוד $s \in \mathbf{Z}_N$, נגריל פולינום אקראי מעל $\mathbf{Z}_N$ מדרגה לכל היותר $t-1$ כך ש- $Q(0) = s$ והחלק של המשתמש ה- i הוא $Q(i)$. הוכיחו כי זוהי סכמה t-מתוך-n לחלוקת סוד.

שאלה 2 [30 נקודות]

נסתכל על מערכת חתימה דמוית ElGamal. אלגוריתם יצירת המפתחות הוא כמו במערכת החתימה המקורית. כלומר עבור p ראשוני גדול ו- g יוצר של $\mathbf{Z}_p$ אלגוריתם יצירת המפתחות מגריל $b \in \{1,...,p-2\}$ ומחשב $B = g^b \bmod p$.
מפתח החתימה הפרטי הוא p,g,b ומפתח הוידוא הציבורי הוא p,g,B. חתימה γ,δ על מסמך $m \in \mathbf{Z}_p^*$ היא חוקית אם $\gamma \in \mathbf{Z}_p^*$, $\delta \in \mathbf{Z}_{p-1}$, $\delta \neq 0$ ו-

$$g^{m\delta} B^{\gamma\delta} \equiv \gamma (\bmod p)$$

סעיף א [10 נקודות]

הראו איך חותם המחזיק במפתח הפרטי יכול לייצר חתימה חוקית לכל מסמך $m \in \mathbf{Z}_p^*$.

סעיף ב [4 נקודות]

הסבירו מדוע הוידוא בשיטה החדשה יותר יעיל מהוידוא בשיטה המקורית של ElGamal.

סעיף ג [6 נקודות]

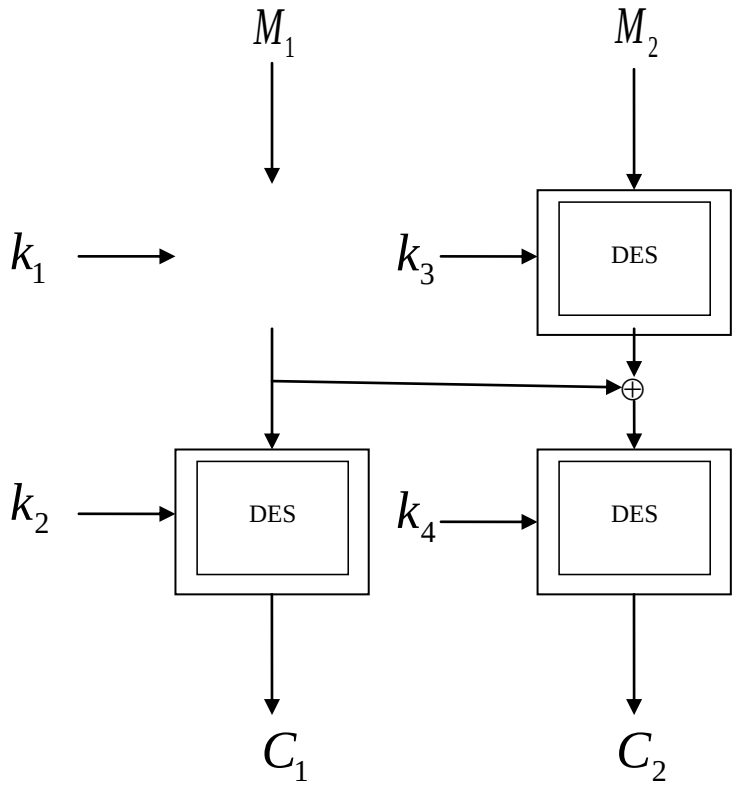
הראו כי ללא ההגבלה $\delta \neq 0$, מתקיף המחזיק במפתח הציבורי יכול לייצר חתימה חוקית לכל מסמך $m \in \mathbf{Z}_p^*$.

סעיף ד [10 נקודות]

הראו התקפה קיומית על שיטת החתימה בשאלה זו. כלומר הראו איך מתוך המפתח הציבורי אפשר לייצר בצורה יעילה הודעה וחתימה חוקית על הודעה.

שאלה 3 [30 נקודות]

נסתכל על מערכת ההצפנה הבאה



במערכת זו, גודל ההודעה והקריפטוגרמה הוא 128 ביטים, וגודל המפתח הוא $56 \cdot 4 = 224$ ביטים.

סעיף א [8 נקודות]

הראן איך מפענח המחזיק במפתחות k_1, k_2, k_3, k_4 יכול לפענח קריפטוגרמה C_1, C_2.

סעיף ב [10 נקודות]

מתקיף מקבל הודעה M_1, M_2 והצפנה שלה C_1, C_2. הראו התקפת חיפוש ממצה על המערכת המשתמשת ב- $2 \cdot 2^{112}$ הפעלות של DES וב- $O(1)$ זכרון.

סעיף ג [12 נקודות]

מתקיף מקבל הודעה M_1, M_2 והצפנה שלה C_1, C_2. הראו התקפת חיפוש ממצה על המערכת המשתמשת ב- $4 \cdot 2^{56}$ הפעלות של DES וב- 2^{56} זכרון.