אוניברסיטת בן-גוריון בנגב
Ben-Gurion University of the Negev
The University celebrates its 30th Anniversary

המחלקה למדעי המחשב

דר' עמוס ביימל

קריפטוגרפיה - מועד א'

202-1-5351

סמסטר ב' תשס"א

3.7.2001

הנחיות:

1. בטופס הבחינה שתי 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.

בהצלחה!

שאלה 1 [20 נקודות]

בשאלה זו נגדיר הכללה של סכמות לחלוקת סוד. יהיו t,k שלמים כך ש- $0 \le k < t$. סכמת (t,k)-לחלוקת סוד היא סכמה שבה מחלקים סוד s בין n משתתפים כך ש:

1. כל קבוצה של משתתפים בגודל לפחות t יכולה לשחזר את הסוד.
2. כל קבוצה בגודל לכל היותר k לא יודעת דבר על הסוד.

לדוגמא, הסכמה של שמיר לחלוקת סוד היא סכמה $(t,t\text{-}1)$-לחלוקת סוד והסכמה של רבין לפיזור מידע היא סכמה $(t,0)$-לחלוקת סוד. שימו לב: בסכמה (t,k)-לחלוקת סוד אין שום דרישה על המידע שבידי קבוצות בגודל בין $k+1$ לבין $t\text{-}1$.

סעיף א [10 נקודות]

בסעיף זה נתאר סכמה נוספת עבור הבעיה של פיזור מידע:
יהי p ראשוני כך ש- $p > n+t$. בהינתן סוד $s = s_1,\ldots,s_t$ כאשר כל $s_i \in \mathbb{Z}_p$ עבור $i=1,\ldots,t$, המחלק מחשב את הפולינום $Q(x)$ מעל $\mathbb{Z}_p$ מדרגה לכל היותר $t\text{-}1$ כך ש- $Q(i+n)=s_i$ עבור $i=1,\ldots,t$. החלק של מעבד i הוא $Q(i)$ עבור $i=1,\ldots,n$.

בסכמה הנ"ל חולק הסוד $s = s_1\ s_2\ s_3$ כאשר $n = 6,\ t = 3$ ו- $p= 11$. החלק של מעבד 2 הוא 7, החלק של מעבד 3 הוא 5 והחלק של מעבד 5 הוא 1. הראו כיצד המעבדים 2,3,5 משחזרים את הסוד.

סעיף ב [10 נקודות]

תארו סכמה (t,k)-לחלוקת סוד בה הסוד הוא איבר ב- $(\mathbb{Z}_p)^{t-k}$ וכל חלק הוא איבר ב- $\mathbb{Z}_p$. יש להוכיח את נכונות הסכמה.

שאלה 2 [30 נקודות]

יהיו p ו- q ראשוניים גדולים שונים זה מזה ו- $N=pq$. נסמן $\lambda(N) = \dfrac{(p-1)(q-1)}{\gcd(p-1,q-1)}$.

סעיף א [10 נקודות]

הוכיחו כי לכל $a \in \mathbb{Z}_N^*$ מתקיים $a^{\lambda(N)} \equiv 1 \pmod N$.

סעיף ב [10 נקודות]

יהיו g_p יוצר של $\mathbb{Z}_p^*$ ו- g_q יוצר של $\mathbb{Z}_q^*$. כמו כן, יהי $g \in \mathbb{Z}_N^*$ כך ש- $g \equiv g_p \pmod p$ ו- $g \equiv g_q \pmod q$. הוכיחו כי הסדר של g ב- $\mathbb{Z}_N^*$ הוא $\lambda(N)$.

סעיף ג [10 נקודות]

נניח כי בוב מחזיק מפתח RSA פרטי N,d והמפתח הציבורי שלו הוא N,e. איב שיחדה את בוב וקיבלה את $\lambda(N)$. הוכיחו כי איב המחזיקה ב- $\lambda(N)$ ובמפתח הציבורי של בוב יכולה לפענח ביעילות כל הודעה שמוצפנת במפתח הציבורי של בוב.

שאלה 3 [25 נקודות]

בשאלה זו נסתכל על מערכת חתימה הדומה למערכת החתימה של ElGamal. אלגוריתם יצירת המפתחות הוא בדיוק כמו באלגוריתם של ElGamal: יהי p ראשוני גדול ו- g יוצר של $\mathbb{Z}_p^*$.

בוב מגריל $b \in \mathbb{Z}_{p-1}^*$ ומחשב $B \leftarrow g^b \mod p$.

מפתח החתימה הוא (p,g,b) ומפתח הוידוא הוא (p,g,B).

אלגוריתם הוידוא:

חתימה על מסמך $M \in \mathbb{Z}_p^*$ היא זוג (γ,δ) כך ש- $B^\delta \gamma^\gamma \equiv g^M \pmod p$.

סעיף א [12 נקודות]

הראו איך בוב יכול לחתום ביעילות על כל מסמך $M \in \mathbb{Z}_p^*$.

סעיף ב [13 נקודות]

הראו כי המערכת אינה עמידה בפני זיוף קיומי.

שאלה 4 [25 נקודות]

נתון זוג M_1, C_1 כאשר $C_1=\mathrm{DES}(M_1,\kappa)$ עבור מפתח κ לא ידוע. התקפת חיפוש ממצה מחפשת את κ על ידי מעבר על כל המפתחות עד שנמצא מפתח $k\in\{0,1\}^{56}$ כך ש- $C_1=\mathrm{DES}(M_1,k)$. בהסתברות גבוהה עבור M ו- C נתונים קיים לכל היותר מפתח k יחיד כך ש- $C=\mathrm{DES}(M,k)$ ולכן $k=\kappa$. התקפה זו דורשת 2^{56} הפעלות של DES.

כדי לחזק את DES כנגד התקפת חיפוש ממצה הוצאו שתי השיטות הבאות:

$$\mathrm{DESV}(M,k,k_1) = \mathrm{DES}(M,k) \oplus k_1$$

$$\mathrm{DESU}(M,k,k_1) = \mathrm{DES}(M \oplus k_1,k)$$

כאשר $k\in\{0,1\}^{56}$ ו- $k_1\in\{0,1\}^{64}$.

סעיף א [4 נקודות]

הראו כיצד מפענחים הודעות ב- DESV ו- DESU כאשר k_1 ו- k נתונים.

סעיף ב [12 נקודות]

נתונים כעת שתי זוגות הודעות M_1,C_1 ו- M_2,C_2 כאשר $C_1=\mathrm{DESV}(M_1,\kappa,\kappa_1)$ ו- $C_2=\mathrm{DESV}(M_2,\kappa,\kappa_1)$ עבור מפתחות κ ו- κ_1 לא ידועים. הראו איך למצוא את κ ו- κ_1 על ידי התקפה הדורשת $2\cdot 2^{56}$ הפעלות של DES. הסתמכו על העובדה כי עבור M_1,M_2 ו- Δ נתונים, בהסתברות גבוהה קיים לכל היותר k יחיד כך ש-

$$\mathrm{DES}(M_1,k) \oplus \mathrm{DES}(M_2,k) = \Delta.$$

סעיף ג [9 נקודות]

הראו כיצד לבצע התקפה דומה עבור DESU. כלומר, נתונים כעת שתי זוגות הודעות M_1,C_1 ו- M_2,C_2 כאשר $C_1=\mathrm{DESU}(M_1,\kappa,\kappa_1)$ ו- $C_2=\mathrm{DESU}(M_2,\kappa,\kappa_1)$ עבור מפתחות κ ו- κ_1 לא ידועים. הראו איך למצוא את κ ו- κ_1 על ידי התקפה הדורשת $2\cdot 2^{56}$ הפעלות של DES.