דר' עמוס ביימל
המחלקה למדעי המחשב

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

קריפטוגרפיה - מועד ב'

202-1-5351

סמסטר ב' תשס"ג

16.7.2003

הנחיות:

1. בטופס הבחינה שני 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 [23 נקודות]

יהיו p ו- q מספרים ראשוניים שונים זה מזה ו- $N=pq$.

סעיף א [10 נקודות]

נתונים שני מספרים A,B המקיימים $A \equiv B \pmod{p}$ אבל $A \neq B \pmod{q}$. הראו איך ניתן לפרק את N ביעילות כאשר נתונים A,B ו- N.

סעיף ב [13 נקודות]

נתונים $e,d \in \mathbb{Z}_N^*$ מספרים כך ש- $ed \equiv 1 (\mathrm{mod}\, \varphi(N))$. תהי $M \in \mathbb{Z}_N^*$ הודעה ו- $C \leftarrow M^e \bmod N$ הצפנה שלה.
מפענח מנסה לפענח את M בצורה הבאה:

1. מחשב $M_p \leftarrow C^d \bmod p$.
2. רוצה לחשב $M_q \leftarrow C^d \bmod q$, אולם טועה בחישוב ומקבל $M'_q \neq M_q \pmod{q}$.
3. מחשב בעזרת משפט השאריות הסיני M' המקיים:
$M' \equiv M_p \pmod{p}$ ו- $M' \equiv M'_q \pmod{q}$.

הראו איך ניתן לפרק את N ביעילות כאשר נתונים M,M' ו- N.

שאלה 2 [25 נקודות]

יהיו p ו- q מספרים ראשוניים שונים זה מזה ו- $N=pq$. נסמן ב- QR_N את קבוצת השאריות הרבועיות מודולו N.

סעיף א [5 נקודות]

הראו כי אם $a,b \in \mathrm{QR}_N$ אזי $a \cdot b \in \mathrm{QR}_N$.

סעיף ב [7 נקודות]

יהיו $a,b \in \mathbb{Z}_N^*$. הראו כי אם $a \in \mathrm{QR}_N$ ו- $b \notin \mathrm{QR}_N$ אזי $a \cdot b \notin \mathrm{QR}_N$.

סעיף ג [13 נקודות]

תזכורת: בשיטת החתימה של רבין, חתימה על מסמך $a \in \mathrm{QR}_N$ היא איבר $s \in \mathbb{Z}_N^*$ המקיים $a \equiv s^2 \pmod{N}$. הראו איך לכל מסמך $a \in \mathrm{QR}_N$ איב יכולה בצורה יעילה לחתום על המסמך על ידי התקפת חתימה נבחרת, כלומר, בהינתן מסמך $a \in \mathrm{QR}_N$ איב יכולה לבקש חתימה על מסמך אחד כרצונה (השונה מ- a) ואח"כ למצוא בצורה יעילה, וללא הסתברות לטעות, חתימה על a.

שאלה 3 [20 נקודות]

סעיף א [12 נקודות]

נתונה מערכת ובה משתמשים משלוש סוגים שונים.

1. n_1 מנהלים שלכל אחד משקל 4.
2. n_2 סגני-מנהלים שלכל אחד משקל 2.
3. n_3 עובדים פשוטים שלכל אחד משקל 1.

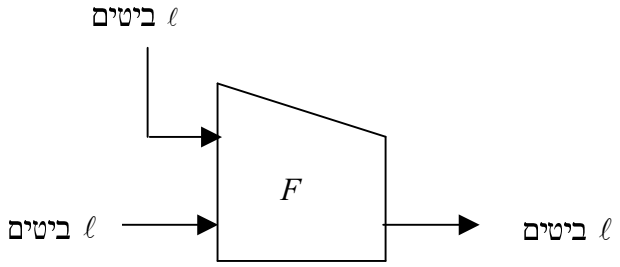
יהי t מספר טבעי. הראו כיצד לממש סכמה יעילה לחלוקת סוד שבה קבוצת משתמשים יכולה לשחזר את הסוד אם ורק אם סכום משקלי המשתתפים בקבוצה הוא לפחות t. יש להוכיח את נכונות הסכמה.

סעיף ב [8 נקודות]

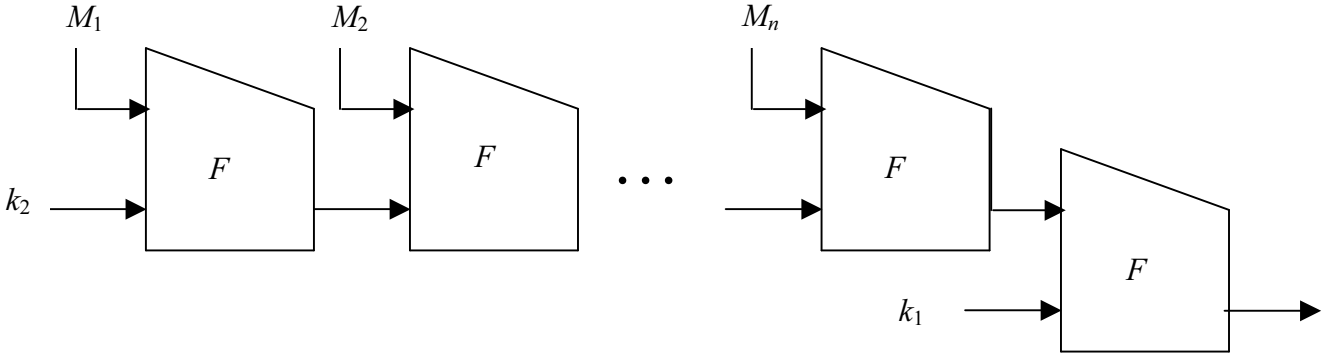
מנהל בסכמה מסעיף א שלח את החלק שלו לכל המשתמשים במערכת. הראו כעת אילו קבוצות יכולות לשחזר את הסוד ואילו קבוצות אינן יכולות לשחזרו.

שאלה 4 [32 נקודות]

בשאלה זו נדון במערכת האותנטיקציה NMAC הבאה (שתוארה בהרצאות). המערכת משתמשת בפונקצית דחיסה $F : \{0,1\}^{\ell} \times \{0,1\}^{\ell} \to \{0,1\}^{\ell}$ המתוארת בציור הבא:



נניח כי לכל $k \in \{0,1\}^{\ell}$ הפונקציה $F(M,k)$, כפונקציה של M, היא פונקציה חד-חד ערכית ועל. הודעה מורכבת ממספר כלשהו של בלוקים, כל אחד באורך ℓ בדיוק. לחשב אותנטיקציה של הודעה המורכבת מ- n בלוקים, כל אחד עם ℓ ביטים, משתמשים ב- $n+1$ פונקציות דחיסה ובמפתח $\langle k_1, k_2 \rangle$ עם 2ℓ ביטים, עפ"י המתואר בציור הבא:



כלומר נגדיר $y_0 \leftarrow k_2$ ו- $y_i \leftarrow F(M_i, y_{i-1})$ והפלט הוא: $\mathrm{NMAC}(\langle M_1,...,M_n \rangle, \langle k_1,k_2 \rangle) = F(y_n, k_1)$. בשאלה זו נראה מדוע ℓ צריך להיות גדול.

סעיף א [8 נקודות]

עבור NMAC עם מפתח $\langle k_1,k_2 \rangle$ ו- n=2, זוג הודעות $\langle M_1,M_2 \rangle$ ן- $\langle M'_1,M'_2 \rangle$ מתנגשות אם

$$\mathrm{NMAC}(\langle M_1,M_2 \rangle, \langle k_1,k_2 \rangle) = \mathrm{NMAC}(\langle M'_1,M'_2 \rangle, \langle k_1,k_2 \rangle).$$

הוכיחו כי אם $\langle M_1,M_2 \rangle$ ו- $\langle M'_1,M'_2 \rangle$ מתנגשות אזי $F(M_2,F(M_1,k_2)) = F(M'_2,F(M'_1,k_2))$.

סעיף ב [8 נקודות]

כמה הודעות עם שני בלוקים יש להגריל מתוך $\{0,1\}^{2\ell}$ כך שבהסתברות לפחות 3/4 נקבל התנגשות?

סעיף ג [8 נקודות]

הוכיחו כי אם $F(M_2,F(M_1,k_2)) = F(M'_2,F(M'_1,k_2))$ אזי לכל M_3 מתקיים

$$\mathrm{NMAC}(\langle M_1,M_2,M_3 \rangle, \langle k_1,k_2 \rangle) = \mathrm{NMAC}(\langle M'_1,M'_2,M_3 \rangle, \langle k_1,k_2 \rangle).$$

סעיף ד [8 נקודות]

נסמן ב- S את המספר שחישבתם בסעיף ב. הראו איך אפשר לשבור את NMAC ע"י $O(S)$ הודעות, כלומר השובר יכול לבקש אותנטיקציה של $O(S)$ מסמכים כרצונו ואח"כ למצוא בהסתברות 3/4 הודעה ואותנטיקציה חוקית שלה (כאשר ההודעה אינה אחת מההודעות שעליהם קיבל אותנטיקציה).