דר' עמוס ביימל
המחלקה למדעי המחשב

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

קריפטוגרפיה - מועד א' 202-1-5351

סמסטר ב' תשס"ג 23.6.2003

הנחיות:

1. בטופס הבחינה שלושה דפים מלבד דף זה. ודאו כי כולם נמצאים בידכם.
2. בבחינה 4 שאלות שמשקלן 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 [25 נקודות]

בשאלה זו נראה איך המפענח החוקי יכול לפענח הודעות במערכת ה- RSA בצורה יותר יעילה. יהיו p ו- q מספרים ראשוניים שונים זה מזה בני n ביטים כל אחד, $N=pq$ ו- $e,d \in \mathbb{Z}_N^*$ מספרים עם $2n$ ביטים כל אחד כך ש- $ed \equiv 1 (\mathrm{mod}\, \varphi(N))$. בשאלה זו נחשב סיבוכיות חישוב מדויקת (כלומר, לא חישוב אסימטוטי בעזרת הסימון O( )). לשם כך, נסתכל על קבוע c כך שלכל m ולכל מספר M עם m ביטים סיבוכיות הכפלת שני איברים ב- $\mathbb{Z}_M^*$ היא cm^2 לכל היותר.

סעיף א [6 נקודות]

מה סיבוכיות חישוב של $C^d \bmod N$ כאשר משתמשים באלגוריתם שתואר בהרצאה?

סעיף ב [6 נקודות]

הסבירו בקצרה מדוע קיימים קבועים α_p, α_q המקיימים $M \equiv \alpha_p M_p + \alpha_q M_q (\mathrm{mod}\, N)$ לכל $M \in \mathbb{Z}_N$ כאשר $M_p \leftarrow M \bmod p$ ו- $M_q \leftarrow M \bmod q$. כיצד אפשר לחשב אותם ביעילות כאשר p ו- q נתונים?

סעיף ג [7 נקודות]

ליעל את החישוב, המפענח בזמן הכנת המפתחות מחשב $d_p \leftarrow d \bmod (p-1)$, $d_q \leftarrow d \bmod (q-1)$ ואת הקבועים α_p, α_q מסעיף ב. תהי M הודעה ו- $C \leftarrow M^e \bmod N$. לפענח את הקריפטוגרמה C, המפענח מחשב $M'_p \leftarrow C^{d_p} \bmod p$, $M'_q \leftarrow C^{d_q} \bmod q$ ו- $M' \equiv \alpha_p M'_p + \alpha_q M'_q (\mathrm{mod}\, N)$. הוכיחו כי הפענוח נכון, כלומר $M' = M$.

סעיף ד [6 נקודות]

מהי סיבוכיות החישוב באלגוריתם הפענוח המתואר בסעיף ג?

שאלה 2 [25 נקודות]

נסתכל על הסכמה הבאה לחלוקת סוד t-מתוך-n. יהי p ראשוני כך ש- $p > n$. לחלק סוד $s \in \mathbb{Z}_p$, המחלק מגריל t-1 איברים אקראיים $r_0, r_1, ..., r_{t-2}$ מתוך $\mathbb{Z}_p$, מסתכל על הפולינום $Q(x) = (s \cdot x^{t-1} + \sum_{j=0}^{t-2} r_j \cdot x^j) \bmod p$ ונותן למשתתף i את החלק $Q(i)$.

סעיף א [7 נקודות]

הראו כי כל קבוצה של משתתפים בגודל לפחות t יכולה לשחזר את הסוד בצורה יעילה מתוך החלקים שקיבלה.

סעיף ב [3 נקודות]

נסתכל על הפולינום $R(x) = (\sum_{j=0}^{t-2} r_j \cdot x^j) \bmod p$. הוכיחו כי אם משתתף i יודע מהו הסוד, אזי הוא יכול לחשב את $R(i)$ מתוך $Q(i)$.

סעיף ג [15 נקודות]

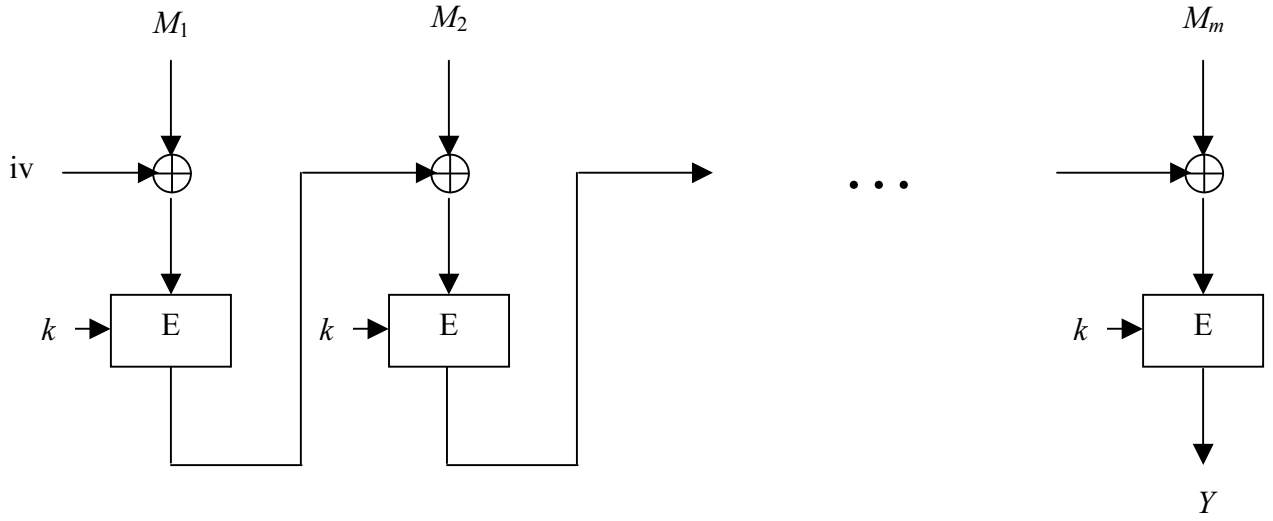
הוכיחו כי כל קבוצה בגודל t-1 לא מקבלת מידע על הסוד מתוך החלקים שלה, כלומר, בהינתן החלקים כל סוד $s \in \mathbb{Z}_p$ אפשרי.

שאלה 3 [25 נקודות]

בשאלה זו נדון בהצעות למערכות אותנטיקציה (MAC) הדומות ל- CBC-MAC אבל אינן טובות.

סעיף א [13 נקודות]

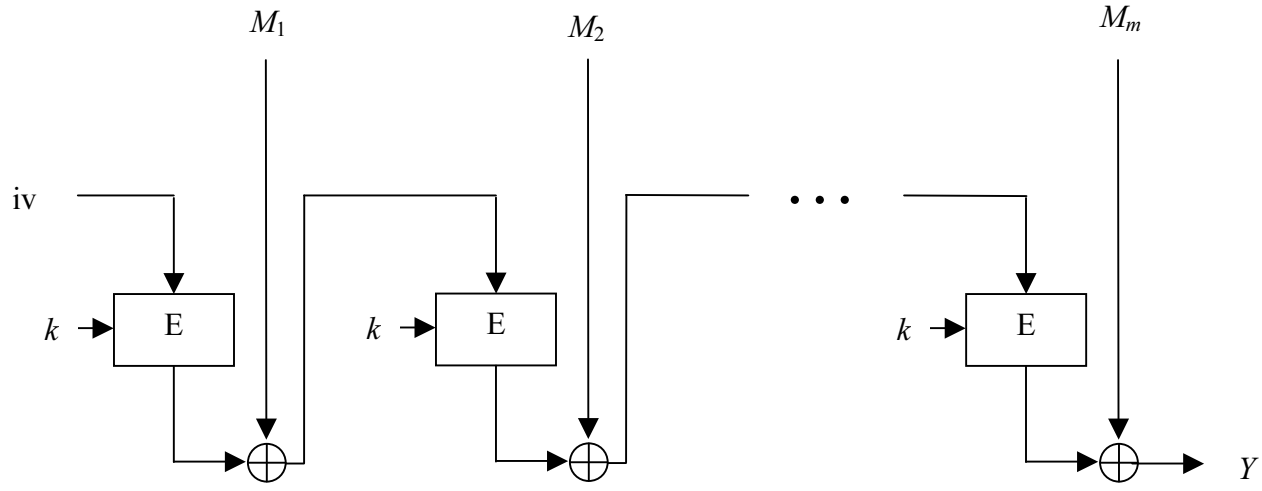
בשיטת האותנטיקציה CBC-MAC הוקטור ההתחלתי (Initial Vector) מוגדר כוקטור שכולו אפסים. נציע את שיטת CBC-MAC1 בה הוקטור ההתחלתי iv נבחר באקראי והוא חלק מהפלט. כלומר, על הודעה $\langle M_1, M_2, ..., M_m \rangle$ הפלט הוא $\langle \text{iv}, Y \rangle$, כאשר Y מחושב על-פי המתואר בתרשים הבא, בו E היא מערכת הצפנה סימטרית עם מפתח k.



בהינתן הודעה $\langle M_1, M_2, ..., M_m \rangle$ והאותנטיקציה שלה $\langle \text{iv}, Y \rangle$, הראו איך ליצר בצורה יעילה הודעה שונה ואותנטיקציה חוקית שלה (ללא הפעלות נוספות של המערכת).

סעיף ב [12 נקודות]

נציע את שיטת BAD-MAC בה הוקטור ההתחלתי iv הוא הוקטור שכולו אפסים ועל הודעה $\langle M_1, M_2, ..., M_m \rangle$ הפלט הוא Y, כאשר Y מחושב על-פי המתואר בתרשים הבא.



בהינתן זוג הודעה $\langle M_1, M_2, ..., M_m \rangle$ והאותנטיקציה שלה Y, הראו איך ליצר בצורה יעילה הודעה שונה ואותנטיקציה חוקית שלה (ללא הפעלות נוספות של המערכת).

שאלה 4 [25 נקודות]

בשאלה זו נראה פרוטוקול דומה לפרוטוקול של Diffie & Hellman. יהי q ראשוני גדול כך ש- $p=2q+1$ ראשוני, g יוצר של $\mathbb{Z}_p^*$ ו- $h \equiv g^2 \bmod p$. נסתכל על החבורה $H_q = \{h^i \bmod p : 1 \le i \le q\}$. תזכורת: לכל $\alpha \in H_q$ מתקיים $\alpha^j \equiv \alpha^{j \bmod q} \bmod p$ לכל מספר טבעי j.

בפרוטוקול החדש אליס מגרילה x באקראי מתוך $\mathbb{Z}_q^*$, מחשבת $X \leftarrow h^x \bmod p$ ושולחת X לבוב. בוב מגריל y באקראי מתוך $\mathbb{Z}_q^*$, מחשב $Z \leftarrow X^y \bmod p$ ושולח Z לאליס. המפתח המשותף הוא $Y \leftarrow h^y \bmod p$.

סעיף א [6 נקודות]

הראו איך אליס יכולה לחשב בצורה יעילה את המפתח המשותף Y כאשר נתונים לה x ו- Z.

סעיף ב [4 נקודות]

נניח (בשלילה) שקיים אלגוריתם יעיל ALG ששובר את הפרוטוקול החדש. כלומר, אם נגריל x,y באקראי מתוך $\mathbb{Z}_q^*$ נחשב $X \leftarrow h^x \bmod p,\ Z \leftarrow h^{xy} \bmod p$ וניתן ל- ALG את הקלט X, Z אזי בהסתברות גבוהה הוא ימצא את $h^y \bmod p$. הראו כי אם נגריל x,z באקראי מתוך $\mathbb{Z}_q^*$, נחשב $X \leftarrow h^x \bmod p,\ Z \leftarrow h^z \bmod p$ וניתן ל- ALG את הקלט X, Z אזי בהסתברות גבוהה הוא ימצא את $h^{x^{-1}z \bmod q} \bmod p$.

סעיף ג [7 נקודות]

נשתמש באלגוריתם ALG כדי לבנות אלגוריתם ALG1 ששובר את הפרוטוקול של Diffie & Hellman בחבורה H_q. הקלט של ALG1 הוא A, B, כאשר $A \equiv h^a \bmod p,\ B \equiv h^b \bmod p$ עבור a,b הנבחרים באקראי מתוך $\mathbb{Z}_q^*$. הפלט הרצוי של ALG1 הוא $h^{ab} \bmod p$. בשלב ראשון ALG1 מגריל c באקראי מתוך $\mathbb{Z}_q^*$, מחשב $C \equiv h^c \bmod p$ ומפעיל את ALG על A,C. הראו כיצד ALG1 יכול לחשב בצורה יעילה את $h^{a^{-1} \bmod q} \bmod p$ מתוך c והפלט של ALG.

סעיף ד [8 נקודות]

בשלב השני ALG1 מפעיל שוב את ALG. הראו על אילו קלטים ALG1 צריך להפעיל את ALG כך שיוכל לחשב את $h^{ab} \bmod p$ בהסתברות גבוהה.