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

קריפטוגרפיה - מועד א'

202-1-5351
סמסטר ב' תשס"ז
25.7.2007

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 [46 נקודות]

נגדיר מערכת RSA כפולה בצורה הבאה:

אלגוריתם יצירת המפתחות:

1. הגרל 4 מספרים ראשוניים גדולים p_1, p_2, q_1, q_2 וחשב $N_1 = p_1 q_1$ ו- $N_2 = p_2 q_2$. אם $N_1 \geq N_2$ לך ל 1.
2. הגרל $e_1 \in \mathbf{Z}^*_{\varphi(N_1)}$ ו- $e_2 \in \mathbf{Z}^*_{\varphi(N_2)}$ וחשב $d_1 = e_1^{-1} \bmod \varphi(N_1)$ ו- $d_2 = e_2^{-1} \bmod \varphi(N_2)$.

מפתח הצפנה ציבורי: N_1, N_2, e_1, e_2.

מפתח פענוח פרטי: N_1, N_2, d_1, d_2.

אלגוריתם ההצפנה:

קלט: $M \in \mathbf{Z}^*_{N_1}$.

1. חשב $C_1 = M^{e_1} \bmod N_1$.
2. חשב $C_2 = C_1^{e_2} \bmod N_2$.

פלט: $\mathrm{DRSA}(M, (N_1, N_2, e_1, e_2)) = C_2$.

סעיף א [6 נקודות]

הראו איך מפענח המחזיק במפתח הפענוח הפרטי יכול לפענח נכון כל הודעה שהוצפנה במפתח ההצפנה הציבורי.

הניחו כי $C_1 \in \mathbf{Z}^*_{N_2}$.

סעיף ב [8 נקודות]

הראו כי אלגוריתם יצירת המפתחות רץ בזמן פולינומי בממוצע.

מטרת הסעיפים הבאים היא להראות כי DRSA אינה מקיימת את תכונת הכפליות. ניקח $A, B \in \mathbf{Z}^*_{N_1}$ המקיימים:

1. $A^{e_1} \equiv 2 (\bmod N_1)$.
2. $B^{e_1} \bmod N_1 > \frac{N_1}{2}$ ו- $B^{e_1} \bmod N_1 \in \mathbf{Z}^*_{N_2}$.

סעיף ג [12 נקודות]

נסמן $C = A \cdot B \bmod N_1$ ו- $D = B^{e_1} \bmod N_1$. הראו כי $\mathrm{DRSA}(C, (N_1, N_2, e_1, e_2)) = (2D - N_1)^{e_2} \bmod N_2$.

סעיף ד [12 נקודות]

הראו כי $\mathrm{DRSA}(A, (N_1, N_2, e_1, e_2)) \cdot \mathrm{DRSA}(B, (N_1, N_2, e_1, e_2))) \equiv (2D)^{e_2} (\bmod N_2)$.

סעיף ה [8 נקודות]

הוכיחו כי $\mathrm{DRSA}(C, (N_1, N_2, e_1, e_2)) \neq (\mathrm{DRSA}(A, (N_1, N_2, e_1, e_2)) \cdot \mathrm{DRSA}(B, (N_1, N_2, e_1, e_2)))(\bmod N_2)$.

שאלה 2 [30 נקודות]

נגדיר את הסכמה הבאה לחלוקת סוד 2-מתוך-2.

קלט: סוד $s \in \{0,1\}$.

1. אם $s = 0$ אזי הגרל $a \in \{0,1\}$ בהתפלגות אחידה.
2. אם $s = 1$ אזי $a = 2$.
3. הגרל $s_1 \in \mathbf{Z}_3$ בהתפלגות אחידה וחשב $s_2 = (a - s_1) \bmod 3$.

פלט: החלק של משתתף 1 הוא s_1 והחלק של משתתף 2 הוא s_2.

סעיף א [6 נקודות]

הוכיחו כי הסכמה הנ"ל היא סכמה לחלוקת סוד 2-מתוך-2. כלומר הסבירו כיצד ניתן לשחזר את הסוד משני החלקים ומדוע לא ניתן ללמוד מידע על הסוד מחלק אחד.

סעיף ב [9 נקודות]

נאמר כי משתתף 1 הצליח לרמות אם הוא שינה את החלק שלו כך שהסוד המשוחזר מהחלק החדש שלו והחלק המקורי של משתתף 2 שונה מהסוד שחולק על ידי המחלק. הראו כי בסכמה שתוארה למעלה משתתף 1 יכול לרמות בהסתברות לכל היותר 0.5 כאשר $s = 0$.

סעיף ג [6 נקודות]

כעת נחלק את אותו הסוד k פעמים באופן בלתי תלוי בעזרת הסכמה שתוארה למעלה. הוכיחו כי סכמה זו היא סכמה לחלוקת סוד 2-מתוך-2.

סעיף ד [9 נקודות]

הוכיחו כי בסכמה מסעיף ג משתתף 1 יכול לרמות בהסתברות לכל היותר $(0.5)^k$ כאשר $s = 0$.

שאלה 3 [24 נקודות]

נסתכל על מערכת אותנטיקציה CBC-MAC עבור הודעות עם שני בלוקים כמו שתוארה בכיתה. כלומר, נשתמש במערכת הצפנה סימטרית E עם הודעות וקריפטוגרמות עם n ביטים, ונבחר עבורה מפתח K. עבור הודעה (M_1, M_2) (כאשר כל M_i הוא עם n ביטים) נגדיר:

$$\text{CBC-MAC}((M_1, M_2), K) = E(E(M_1, K) \oplus M_2, K).$$

תזכורת: התנגשות היא זוג הודעות (M_1, M_2) ו- (M'_1, M'_2) כך ש- $(M_1, M_2) \neq (M'_1, M'_2)$ אבל $\text{CBC-MAC}((M_1, M_2), K) = \text{CBC-MAC}((M'_1, M'_2), K)$.

סעיף א [4 נקודות]

נשתמש ב- CBC-MAC כאשר מערכת ההצפנה היא DES. כמה הודעות יש להגריל כדי שנמצא התנגשות בהסתברות 0.75?

סעיף ב [10 נקודות]

נגדיר את מערכת ההצפנה WDES אשר גודל ההודעות והקריפטוגרמות בה הוא 128 ביטים וגודל המפתח הוא 112 ביטים. עבור הודעה $M = (A, B)$ כאשר A ו- B הן מחרוזות בנות 64 ביטים כל אחת ומפתח $K = (K_1, K_2)$ כאשר K_1 ו- K_2 הן מחרוזות בנות 56 ביטים כל אחת, נגדיר

$$\text{WDES}((A, B), (K_1, K_2)) = \text{DES}(A, K_1), \text{DES}(B, K_2).$$

נשתמש ב- CBC-MAC כאשר מערכת ההצפנה היא WDES. כמה הודעות יש להגריל כדי שנוכל לייצר התנגשות בהסתברות 0.75?

סעיף ג [10 נקודות]

נגדיר את מערכת ההצפנה 'WDES אשר גודל ההודעות בה הוא 64 ביטים, גודל הקריפטוגרמות בה הוא 128 ביטים וגודל המפתח הוא 112 ביטים. עבור הודעה M כאשר M היא מחרוזת בת 64 ביטים ומפתח $K = (K_1, K_2)$ כאשר K_1 ו- K_2 הן מחרוזות בנות 56 ביטים כל אחת, נגדיר

$$\text{WDES}'(M, (K_1, K_2)) = \text{DES}(M, K_1), \text{DES}(M, K_2).$$

עבור K_1 ו- K_2 נתונים, מהו מספר הפלטים האפשריים של 'WDES? נשתמש במערכת דמויית CBC-MAC הבאה:

$$\text{WDES}'(\text{DES}(M_1, K) \oplus M_2, K_1, K_2).$$

כמה הודעות יש להגריל כדי שנוכל לייצר התנגשות בהסתברות 0.75?