שאלה 5 (20 נקודות)

בשאלה זו נדון בשיטות אימות נכונות של הודעות (כלומר הגנה מפני שינוי הודעות ע"י חבלנים, מבלי שמקבל ההודעה יבחין בחבלה). ההודעות יכולות להיות ארוכות, ומוסיפים תוספת קצרה המבטיחה אימות. לתוספת זו קוראים Message Authentication Code או בקיצור MAC.

תזכורת:

שיטת ה - Hashing של רבין:

בהנתן הודעה $M = m_1 m_2 \ldots m_\ell$, כאשר $m_i \in \{0,1\}^{56}$ ו - S הודעה סטנדרטית, $H_0(M)$ מוגדר ע"י:

$$n_1 = \mathrm{DES}(S, m_1)$$

$$n_2 = \mathrm{DES}(n_1, m_2)$$

$$\vdots$$

$$n_\ell = \mathrm{DES}(n_{\ell-1}, m_\ell) = H_0(M)$$

הערה: בשאלה זו נתעלם מהתקפות בשיטת פרדוקס יום ההולדת, שעליהן ניתן להתגבר ע"י הגדלת המילים שאותן מצפינים.

תהי $\mathrm{SIG}_A(M)$ שיטת חתימה (במפתח ציבורי) של משתמש A על הודעה M. נניח ש - A הוא שולח ההודעה. נגדיר $\mathrm{MAC}_1(M) = \mathrm{SIG}(H_0(M))$.

(3%) א. הסבר מדוע MAC_1 מגינה בפני יכולתו של חבלן Z לשלוח ל - B הודעה אחרת כך ש - B יאמין שההודעה נשלחה ע"י A.

היות ושיטות חתימה הינן יקרות, נבחן את האפשרות לשימוש במפתח סודי (הידוע רק ל - A ול - B) לצורך בניית MAC.

(10%) ב. יהיה $H_1(M, K_1)$ מוגדר כמו H_0 בהבדל שבמקום S משתמשים במפתח סודי $K_1 \in \{0,1\}^{64}$. אם נשתמש ב - $\mathrm{MAC}_2(M) = H_1(M, K_1)$, האם Z יכול לייצר $\mathrm{MAC}_2(M')$ עבור $M' \neq M$ בהנתן $\mathrm{MAC}_2(M)$? נמק.

(7%) ג. נגדיר $\mathrm{MAC}_3(M, K_2) = \mathrm{DES}(H_0(M), K_2)$, כאשר $K_2 \in \{0,1\}^{56}$ הוא מפתח סודי (הידוע רק ל - A ול - B). האם Z יכול לשנות את M במקרה זה ?

שאלה 4 (30 נקודות)

תזכורת:

הפרוטוקול של Fiat-Shamir להזדהות (authentication):

יהיו p, q ראשוניים גדולים שאינם ידועים למשתמשים, ו - $N = p \cdot q$ ידוע למשתמשים.

הכנה: המוכיח מגריל $S \in Z_N^*$, ומפקיד את $I = S^2 \bmod N$ בקובץ הציבורי.

הפרוטוקול:

1. המוכיח בוחר מס' אקראי R שמקיים $1 < R < N$.
2. המוכיח מחשב את $X = R^2 \bmod N$, ושולח את X למוודא.
3. המוודא מבקש מהמוכיח את $R \bmod N$ או את $RS \bmod N$ (אך לא את שניהם).
4. המוכיח שולח למוודא את המידע שביקש.
5. המוודא בודק האם מתקיים $R^2 = X \bmod N$ או $(RS)^2 = XI \bmod N$, בהתאם לבקשתו ב - 3.

הוצע להחליף בשלב 2 של הפרוטוקול את $X = R^2 \bmod N$ בהגרלת מס' אקראי $0 \le m < N$, וחישוב $X = R^2 + mN$.

(2%) א. הסבר בקצרה מדוע קל למצוא שורש ריבועי של R^2 (ללא רדוקציה מודולרית).

(3%) ב. הסבר מדוע בהנתן X, כמו בפרוטוקול המקורי, אי אפשר להשתמש בשיטה מסעיף א למציאת שורש ריבועי מודולו N.

(15%) ג. הוכח שבתחום $0 < Y < N^2$ יש בדיוק 4 מספרים שלמים (שונים) Y_1, Y_2, Y_3, Y_4 שיש להם שורש ריבועי שלם (ללא רדוקציה מודולרית), המקיימים $Y_i = R^2 \bmod N$.

(8%) ד. תן חסם על ההסתברות שהערך X, לפי ההצעה, יהיה מספר שיש לו שורש שלם (ללא רדוקציה).
רמז: שים לב לתחום האפשרי ל - X, לפי ההצעה.

(2%) ה. בהנחה שביצוע כפל זול יותר מביצוע חילוק, הסבר את היתרון של ההצעה.

שאלה 1 (10 נקודות)

לשם העברת קבצים בשפה האנגלית בין A לבין B בתווך לא מוגן הוצע להשתמש בצופן אקראי $E : \{0,1\}^{100} \to \{0,1\}^{100}$. כל תו m_i (בתחום $0 - 25$) מוצפן ע"י: $c_i = E(m_i)$ ומפוענח ע"י $m_i = D(c_i)$, כאשר D היא פונקציית הפענוח של הצופן.

(3%) א. מדוע צופן זה אינו עמיד בפני נסיונות פיצוח ?

(7%) ב. בהנחה שמצפינים כל אות בנפרד, איך ניתן לתקן את המערכת לקבלת צופן בטוח ?

שאלה 2 (20 נקודות)

(8%) א. הוכח שעבור p ראשוני, אם α יוצר (איבר פרימיטיבי) של Z_p^*, אזי הסדר של $\beta = \alpha^i$ הוא $\frac{p-1}{\gcd(p-1,i)}$.

(12%) ב. עבור צופן כלשהו, עם מפתח k, הודעה M נקראת קבועה אם $E(M,k) = M$.
הוכח שבמערכת RSA, עם מודולו $n = pq$ ומפתח פומבי (n,e), מס' ההודעות הקבועות הוא $\gcd(p-1, e-1) \cdot \gcd(q-1, e-1)$.

שאלה 3 (20 נקודות)

בשאלה זו נצפין הודעות באורך 256 ביט תוך שימוש חוזר ב - DES, עם מפתח אחד בן 56 ביטים.
ההודעה תהיה $M_1M_2M_3M_4$, כאשר כל M_i הוא מאורך 64 ביטים.
נעיין בשלוש השיטות הבאות:

- Electronic Code Book mode (ECB): $C_i = \mathrm{DES}(M_i, k)$.
- Cipher Block Chaining mode (CBC): $C_i = \mathrm{DES}(M_i \oplus C_{i-1}, k)$, כאשר $C_0 = \mathrm{S}$.
- Output FeedBack mode (OFB): $C_i = M_i \oplus V_i$, כאשר $V_i = \mathrm{DES}(V_{i-1}, k)$, וכן $V_0 = \mathrm{S}$.

כאשר S היא הודעה סטנדרטית והקריפטוגרמה היא $C_1C_2C_3C_4$.

(10%) א. נניח ש - A ו - B הסכימו על מפתח k. A משתמש ב - k להצפנת הודעה x באורך 256 ביטים ושולח אותה ל - B. נסמן את ההודעה המוצפנת ב - y.
בדרך בין A ל - B הביט ה - 80 של y התהפך, כלומר B מקבל קריפטוגרמה y' ששונה מ - y בביט ה - 80 שלה. B מפענח את y' ומקבל את x'.
לכל אחד משלושת ה - modes, אילו ביטים של x' ישארו זהים לביטים המתאימים בהודעה x (לכל plaintext).

(10%) ב. יהיו x ו - x' הודעות באורך 256 ביטים השונות רק בביט ה - 80. יהיו y ו - y' ההצפנות של x ו - x' בהתאמה. לכל אחד משלושת ה - modes, אילו ביטים של y' ישארו זהים לביטים המתאימים ב - y.

הטכניון - מכון טכנולוגי לישראל
הפקולטה למדעי המחשב
20.3.98

פרופ' שמעון אבן
דרור רביץ

מבחן מועד ב'
קריפטולוגיה מודרנית
חורף תשנ"ח

הנחיות:

1. הבחינה עם חומר פתוח.
2. בטופס הבחינה 3 דפים מלבד דף זה. וודא כי כולם בידך.
3. בבחינה 5 שאלות שמשקלן אינו שווה. יש לענות על כולן.
4. הוכח את כל תשובותיך. פתרון ללא הוכחה לא יתקבל.
5. הנך רשאי להסתמך על סעיפים קודמים, גם אם לא השבת עליהם.
6. משך הבחינה – 3 שעות. השתדל לצבור מקסימום נקודות בזמן הקצוב.

בהצלחה!