הטכניון – מכון טכנולוגי לישראל הפקולטה למדעי המחשב

5.3.2000

פרופ' שמעון אבן
אור דונקלמן

קריפטולוגיה מודרנית – 236506
מבחן מועד ב'
חורף תש"ס

הנחיות:

- הבחינה עם חומר פתוח.
- נמק/י את כל תשובותיך, תשובה לא מנומקת לא תזכה בנקודות.
- כתוב/כתבי בצורה מסודרת ונקיה ובכתב ברור. תשובות לא ברורות לא תיבדקנה.
- בבחינה 5 שאלות, משך הבחינה שלוש שעות.

בהצלחה !

שאלה מס' 1 (10%)

תהא T מערכת הצפנה קונוונציונאלית שבה n הודעות, n קריפטוגרמות ו-n מפתחות.
הוכח ש- T פרפקטית אם מתקיימים שני התנאים הבאים:

- לכל הודעה M, וקריפטוגרמה C, קיים מפתח K שעבורו E(M,K)=C.
- כל המפתחות שווי הסתברות.

שאלה מס' 2 (15%)

ברשת שבה נתונה שיטת רבין להצפנה (תזכורת: לכל משתמש U יש מפתח ציבורי n_U שהוא מכפלה של שני מספרים ראשוניים גדולים p_U ו- q_U. בהנתן הודעה $1 \le M < n_U$, ההצפנה במפתח הציבורי של U הינה $(E_U(M) = [M^2]_{n_U}$ משתמש S שולח אותה הודעה M לשני משתמשים אחרים, A ו-B.
בהנחה שמתקיימים התנאים הבאים:

- $1 \le M < \min\{n_A, n_B\}$,
- $\gcd\{n_A, n_B\} = 1$,
- משתמש T שומע את $E_A(M)$ ואת $E_B(M)$.

הראה ש-T יכול לחשב, ביעילות, את M.
רמז: $M^2 < n_A \cdot n_B$

שאלה מס' 3 (20%)

בשאלה זו p הוא ראשוני גדול. g הוא גנרטור של Z_p^*. שניהם ידועים לכל.

בעיית Diffie-Hellman (להלן DHP):
בהנתן $[g^x]_p$ ו- $[g^y]_p$, כאשר $1 \le x, y \le p-2$ (שנבחרו באקראי), חשב את $[g^{xy}]_p$.

במערכת המפתח הציבורי של ElGamal:

- כל משתמש A בוחר באקראי $1 \le a \le p-1$ מחשב את $[g^a]_p$ ומפרסמו כמפתח ציבורי.
- כאשר B רוצה לשלוח הודעה $m \in Z_p$ הוא בוחר באקראי $1 \le k \le p-2$, מחשב את:

$$\gamma = [g^k]_p$$
$$\delta = [m \cdot (g^a)^k]_p$$

ושולח את (γ, δ) ל-A.

בעיית הפיצוח של ElGamal (להלן EGP):
בהנתן הקריפטוגרמה (γ,δ) חשב את m.

הוכח כי DHP ו-EGP שקולות.

שאלה מס' 4 (20%)

שאלה זו דנה בפרוטוקול דואר רשום.
ל-A יש הודעה M המיועדת ל-B. Aמעוניין בחתימה של B המאשרת כי B קבל את M. B מעוניין לקבל את M .
מטרת הפרוטוקול להבטיח שגם A וגם B יהיו מרוצים, מבלי שאחד יקופח בעוד השני יהיה מרוצה.
P(A,B):

- A בוחר באקראי $K,\alpha_1,\alpha_2,\ldots,\alpha_n \in \{0,1\}^{56}$.
- A מחשב עבור כל i $\alpha_i' = \alpha_i \oplus K$
- A מחשב את הקריפטוגרמות הבאות:

$$DES(S,K), DES(S,\alpha_1), DES(S,\alpha_2),\ldots, DES(S,\alpha_n),$$
$$DES(S,\alpha_1'), DES(S,\alpha_2'),\ldots, DES(S,\alpha_n'), DES(M,K)$$

עבור S הודעה סטנדרטית ידועה.

- A חותם על ההצהרה: "2n+2 הקריפטוגרמות שלי הן ... (מפרש אותן)".
- B בוחר באקראי $\beta_1,\beta_2,\ldots,\beta_n,\gamma_1,\gamma_2,\ldots,\gamma_n \in \{0,1\}^{56}$
- B מחשב את הקריפטוגרמות:

$$DES(S,\beta_1), DES(S,\beta_2),\ldots, DES(S,\beta_n),$$
$$DES(S,\gamma_1), DES(S,\gamma_2),\ldots, DES(S,\gamma_n),$$

- B חותם על ההצהרה: "2n הקריפטוגרמות שלי הן ... (מפרש אותן). אם A יודע זוג אחד, (β_i,γ_i) אזי קבלתי את M המתאים להצהרת A."

א. איך ניתן להמשיך בפרוטוקול על מנת להשיג את המטרה? (10%)
ב. הסבר מדוע המטרה אמנם מושגת? (10%)

שאלה מס' 5 (35%)

מתוארת שיטת החתימה המקורית של רבין:

תהליך ההכנה:

כל משתמש U מפקיד בקובץ הציבורי וקטורים מהצורה $V_U = (DES(S,K_1^U), DES(S,K_2^U),\ldots, DES(S,K_{40}^U))$. כאשר $K_1^U, K_2^U,\ldots,K_{40}^U$ הם מפתחות הנבחרים באקראי ו-S היא הודעה סטנדרטית.

תהליך החתימה:

1. בהנתן $M \in \{0,1\}^{64}$ שעליה רוצה A לחתום בפני B, A מכין וקטור $W = (DES(M,K_1^A), DES(M,K_2^A),\ldots,DES(M,K_{40}^A))$, כאשר המפתחות $K_1^A, K_2^A,\ldots,K_{40}^A$ מתאימים לוקטור V_A, ושולח את W ל-B.
2. B בוחר באקראי וקטור $I \subseteq \{1,2,\ldots 40\}$ בן 20 איברים ושולח ל-A.
3. A מגלה את $\{K_i^A \mid i \in I\}$.

תהליך אימות החתימה:

4. B בודק האם הערכים $\{DES(S,K_i^A) \mid i \in I\}$ מתאימים לאיברים מתוך V_A.
5. B בודק האם הערכים $\{DES(M,K_i^A) \mid i \in I\}$ מתאימים לאיברים מתוך W.

במידה ואין התאמה באחת הבדיקות (4 או 5), B דוחה את החתימה.

יותר מאוחר אם A מתכחש לחתימתו, B פונה לבית המשפט.

תהליך השיפוט:

6. B מציג את M ואת W.
7. השופט מבקש מ-A לגלות את $K_1^A, K_2^A,\ldots,K_{40}^A$.
8. A מוסר את הערכים.
9. השופט בודק אם כל 40 המפתחות מתאימים ל-V_A. אם אין התאמה מלאה, או ש-A מסרב לגלות את המפתחות פסק הדין מחייב את A.
10. השופט בודק כמה ערכים מתוך $DES(M,K_1^A),\ldots,DES(M,K_{40}^A)$ מתאימים לאלה שנמסרו ע"י B בצעד 6. אם יש 20 התאמות, או פחות, השופט מזכה את A. אם יש 21 התאמות, או יותר, השופט מחייב את A.

א. הסבר מדוע שיטת החתימה היא חד-פעמית. (כלומר אין להשתמש ב-V_A יותר מפעם אחת). (5%)

ב. מה ההסתברות ש-B יוכל לשכנע את C, שאינו שופט, שיש לו חתימה של A על M? (5%)

ג. מה ההסתברות ש-B יוכל לזייף חתימה של A על מסמך אחר M'? (5%)

ד. בהנתן K_i, האם A מסוגל למצוא K המקיים:

$$DES(S,K) = DES(S,K_i)$$

$$K \neq K_i$$

נתח את ההסתברות לקיום K שכזה, ואת הסיבוכיות למציאתו.
הסבר כיצד מציאת K שכזה מסייעת בידי A להתכחש לחתימה. (10%)

ה. אם A בוחר עוד לפני תהליך ההכנה $4 \cdot 2^{32}$ מפתחות אקראיים, האם בהסתברות בלתי זניחה יהיו זוגות של מפתחות K, K' שונים, כך ש-$DES(S,K) = DES(S,K')$?
הראה כיצד ניתן להשתמש בזוגות כאלה על מנת להפקיד בתהליך ההכנה וקטורים שהחתימה בעזרתם ניתנת להכחשה. (10%)