הטכניון – מכון טכנולוגי לישראל הפקולטה למדעי המחשב

17.12.99

פרופ׳ שמעון אבן
אור דונקלמן

קריפטולוגיה מודרנית – 236506
בחן אמצע
חורף תש״ס

הנחיות:

- הבחינה עם חומר פתוח.
- נמקו את כל תשובותיכם, תשובה לא מנומקת לא תזכה בנקודות.
- כתוב בצורה מסודרת ונקיה ובכתב ברור. תשובות לא ברורות לא תיבדקנה.
- בבחינה 4 שאלות, משך הבחינה שעתיים.

בהצלחה !
כולל עדכונים מזמן הבחינה

שאלה מס' 1 (22%)

א. יהי $p>3$ מס' ראשוני ו- $r\in Z^*_p$ הוא Q.R. מודולו p. האם יתכן ש- r, הוא גנרטור (איבר פרימטיבי) ב- Z^*_p ? נמק. (9%)

ב. הוכח שאם ראשוני p מקיים $p\equiv 1 \pmod{16}$ אזי 2 אינו גנרטור של Z^*_p . (13%)

שאלה מס' 2 (23%)

יהי $n=p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}$ כאשר $1<p_1<p_2<\cdots<p_k$

א. הוכח כי $n\geq 2^k$. (2%)

ב. הוכח כי $1-1/p_i\geq 1-1/(i+1)$. (5%)

ג. השתמש בסעיפים הקודמים כדי להראות כי: $\varphi(n) \geq n/(1+\log_2(n))$. (16%)

שאלה מס' 3 (25%)

בשאלה זו נדון בהתקפה על שיטת הצפנה הדומה ל-Vigenère.

ה-plaintext, $p_1,p_2,\ldots,p_L$ כתוב באנגלית רגילה, בהשמטת כל סימני הפיסוק והרווחים. המפתח $K_1,K_2,\ldots,K_m$, אורכו m, כאשר $L>>m$. כמו-כן אנו נניח שערכו של m ידוע לכל.

ה- ciphertext, $C_1,C_2,\ldots,C_L$ מחושב כדלקמן (בהנחה ש-26 אותיות הא"ב מיוצגות ע"י הערכים $0,1,\ldots,25$):

עבור $1 \leq i \leq m$: $C_i = p_i + K_i \pmod{26}$

עבור $m+1 \leq i \leq L$: $C_i = p_i + p_{i-m} \pmod{26}$

א. הסבר כיצד ידיעת ה-ciphertext והמפתח מאפשרים לפענח את ההודעה. (5%)

ב. תאר שיטה לשבירת הצופן והסבר על מה היא מבוססת. (20%)

רמז: עבור $1 \leq i \leq m$, מתוך ידיעת ה-ciphertext וניחוש ערכו של K_i ניתן לחשב גם את $p_i,p_{i+m},p_{i+2m},\ldots,p_{i+[(L-i)/m]*m}$ (איך? ולמה זה עוזר?)

שאלה מס' 4 (30%)

בהנחה ש-F, הוא צופן בלוקים אקראי, עם פרמטרים כמו ב-DES ($\mathbf{M}=\mathbf{C}=\{0,1\}^{64}$, $\mathbf{K}=\{0,1\}^{56}$).

מוצעת שיטת הצפנה כפולה. בשיטה זו מרחבי ההודעות והקריפטוגרמות אינם משתנים, אולם המפתח K הוא בן 112 ביטים $K=(K_1,K_2)$ כאשר $K_1,K_2\in\mathbf{K}$.

בהנתן הודעה $M\in\mathbf{M}$, הקריפטוגרמה C מחושבת ע"י: $C=F(F(M,K_1),K_2)$.

א. הסבר בקצרה מדוע, לכאורה, שיטת ההצפנה הכפולה בטוחה יותר מהצפנה בודדת. (2%)

נדון בשיטה לפיצוח ההצפנה הכפולה, בהנתן היסטוריה (M_1,C_1), (M_2,C_2) המפצח בונה שתי קבוצות:

$\mathbf{S_1}=\{F(M_1,K'_1) \mid K'_1 \in \mathbf{K}\}$

$\mathbf{S_2}=\{F^{-1}(C_1,K'_2) \mid K'_2 \in \mathbf{K}\}$

ואחר כך יוצר את <u>קבוצת הפגיעות הראשונה</u> על ידי:

$\mathbf{T_1}=\{(K'_1,K'_2) \mid F(M_1,K'_1) = F^{-1}(C_1,K'_2)\}$

ב. מהי סיבוכיות המקום והזמן ליצירת $\mathbf{S_1}$, $\mathbf{S_2}$, $\mathbf{T_1}$? (5%)

ג. מהי העצמה הצפויה של $\mathbf{T_1}$? נמק. (9%)

לבסוף, המפצח בונה את <u>קבוצת הפגיעות השניה</u> על ידי:

$\mathbf{T_2}=\{(K''_1,K''_2) \mid (K''_1,K''_2) \in \mathbf{T_1} \text{ and } C_2=F(F(M_2,K''_1),K''_2)\}$

ד. מהי סיבוכיות המקום והזמן ליצירת $\mathbf{T_2}$? (5%)

ה. מהו המספר הצפוי של אברים ב- $\mathbf{T_2}$? (9%)