שאלה מס' 1 (18%)

נתבונן על השלב ה - i ב - DES. עבור קלט מצד ימין R_{i-1} קבוע לשלב זה, כמה בחירות ישנן עבור המפתח K_i בכדי שיתקבל $f\left(R_{i-1}, K_i\right) = 0...0$? נמק.

שאלה מס' 2 (18%)

מפתח K ל - DES נקרא דואלי אם לכל $M \in \{0,1\}^{64}$ מתקיים DES(DES(M,K),K)=M.
הוכח שאם C_0 מכיל רק אפסים, או רק אחדים, וגם D_0 מכיל רק אפסים או רק אחדים, אז K הוא דואלי (C_0 ו - D_0 הם סימונים המתייחסים לאלגוריתם יצירת 16 המפתחות מתוך K).

שאלה מס' 3 (18%)

חשב בדרך היעילה ביותר הידועה לך את התשובה לשאלה הבאה:
האם 1997 הוא שארית ריבועית מודולו המספר הראשוני 6961 ?

שאלה מס' 4 (28%)

נתאר וריאנט של צופן Vigenere:
בהינתן מילת מפתח $K_1K_2\cdots K_m$ מאורך m, נבנה מפתח ע"י הכלל:

$$z_i = K_i \quad (1 \le i \le m)$$

$$z_i = z_{i-m} + 1 \mod 26 \quad (i \ge m+1)$$

כלומר, בכל פעם שאנו משתמשים במילת המפתח, אנו מחליפים כל אות ע"י האות העוקבת אחריה מודולו 26.
למשל, אם מילת המפתח היא SUMMER, אז נשתמש ב - SUMMER להצפנת שש האותיות הראשונות, ונשתמש ב - TVNNFS להצפנת שש האותיות הבאות, וכן הלאה.

(8%) א. תאר איך תשנה את ההתקפה של קסיסקי לפיצוח Vigenere כדי להתקיף צופן זה, כאשר אורך הטקסט הוא פי 10000 מאורך מילת המפתח.

(20%) ב. כנ"ל, כאשר אורך הטקסט הוא פי 100 מאורך מילת המפתח.

שאלה מס' 5 (18%)

הוכח שאם צופן הוא פרפקטי עבור פילוג הסתברותי מסויים של ההודעות, אזי הוא פרפקטי לכל פילוג של ההודעות.

הטכניון - מכון טכנולוגי לישראל הפקולטה למדעי המחשב

12.12.97

פרופ׳ שמעון אבן
דרור רביץ

קריפטולוגיה מודרנית - 236506
בחן אמצע
חורף תשנ״ח

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 5 שאלות, משך הבחינה שעתיים.

בהצלחה !