הטכניון – מכון טכנולוגי לישראל
הפקולטה למדעי המחשב
25.2.01

פרופ/ח אלי ביהם
אור דונקלמן

מבחן מועד א'
קריפטולוגיה מודרנית 236506
חורף תשס"א – מעודכן (הערות מהמבחן)

הנחיות:

1. משך המבחן: 3 שעות.
2. במבחן 4 שאלות. ענה על כולן.
3. מותר להשתמש בכל חומר עזר לא אלקטרוני.
4. כתוב בצורה מסודרת ונקייה בכתב ברור. הוכח את כל תשובותיך.
5. **הקצה מראש 2 עמודים במחברתך לכל שאלה לפי סדר השאלות.**
6. **שים לב: הקדש את 10 הדקות הראשונות לקריאת כל השאלות והבנתן.**

בהצלחה!

שאלה מס' 1 (25 נק')

נקרא לזוג פונקציות $f_1, f_2 : D \to R$ חסרות מפגש אם קשה למצוא $x, y \in D$ כך ש- $f_1(x) = f_2(y)$.

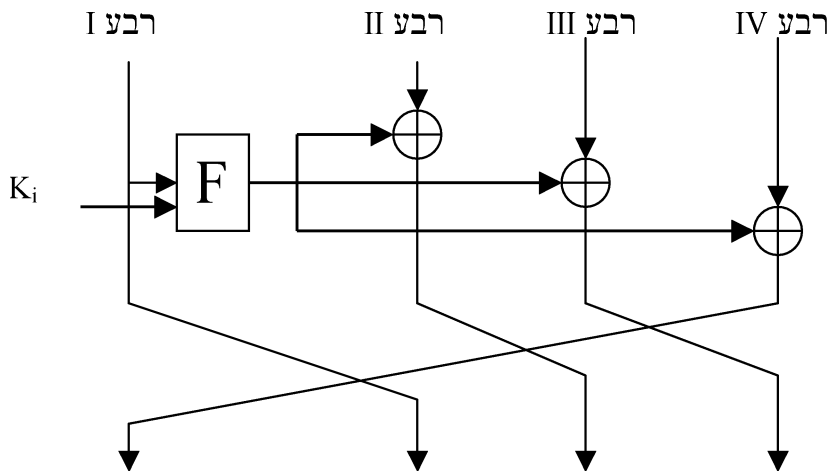
א. יהי p ראשוני, g יוצר של Z_p^* ו- $k \in Z_p^*$, נניח כי בעית ה-DLOG הינה קשה (בהנתן $p, g, y = g^x \bmod p$ קשה למצוא את x).
הוכח כי זוג הפונקציות הבאות f_1, f_2 הינן חסרות מפגש:
$f_1(x) = g^x \bmod p, f_2(x) = k \cdot g^x \bmod p$.

ב. יהי p,q ראשוניים לא ידועים, $n=pq$, $e \in Z_{\varphi(n)}^*$ ו- $m,r \in Z_n^*$, אזי תחת ההנחה שבעיית RSA הינה קשה (בהנתן $e, n, m^e \bmod n$ קשה למצוא את m).
הוכח כי זוג הפונקציות הבאות g_0, g_1 הינן חסרות מפגש:
$g_0(m) = m^e \bmod n, g_1(m) = r \cdot m^e \bmod n$.

ג. בסעיף זה נשתמש ב- g_0, g_1 מהסעיף הקודם.
נגדיר את פונקצית התמצות הבאה – עבור $X = b_{n-1} b_{n-2} \cdots b_0$ (X באורך n *ביטים*)
נגדיר $H(X) = g_{b_{n-1}}(g_{b_{n-2}}(\cdots(g_{b_0}(IV))\cdots))$ כש-IV הינה מחרוזת קבועה (למשל 110110000101011111000111).
לדוגמא - אם X=110 אזי $H(X) = g_1(g_1(g_0(IV)))$.
הוכח ש-H היא פונקצית תמצות חסרת התנגשויות, כלומר בהינתן M_1, M_2 כך ש- $H(M_1) = H(M_2)$ ניתן למצא ביעילות x,y כך ש- $g_0(x) = g_1(y)$.

שאלה 2 (25 נק')

הצופן הבא הוצע כדי לשפר את DES ע"י הגדלת מספר השלבים וגודל הבלוק ללא הקטנת המהירות של ההצפנה (בביטים לשניה).
כעת גודל הבלוק 128 ביטים ומספר השלבים 32, גודל המפתח נותר 56 ביטים. כל בלוק מחולק ל-4 רבעים, כשכל רבע בן 32 ביט.
תהי F פונקציית ה-F של DES.
שלב i של הצופן החדש הינו:



כאשר $K_1,...,K_{32}$ נוצרים ע"י Key Schedule Algorithm דומה (אך לאו דווקא זהה) לזה של DES.

האם צופן זה חזק יותר או חלש יותר מ-DES מבחינת קריפטאנליזה דיפרנציאלית?
תאר את ההתקפה הדיפרנציאלית הטובה ביותר שאתה מוצא כנגד צופן זה,על איזו תכונה היא מסתמכת, מדוע היא פועלת ומה סיבוכיותה.

שאלה 3 (25 נק')

הגדרה: נגדיר קבוצה מסוימת להיות **קבוצה נשמרת** תחת פעולה E, אם לכל איבר x במרחב, מתקיים ש-x בקבוצה אם ורק אם $E(x)$ בקבוצה.
כמו כן נגדיר **קבוצה נשמרת בולטת**, להיות קבוצה נשמרת אשר בהנתן x ניתן לזהות אם x בקבוצה בזמן פולינומיאלי.

א. הוכח כי הקבוצה - $S_1 = \{x \mid x \in Q.R.(p)\}$ כש-p מספר כלשהו, נשמרת כאשר $E(x)=xy$ mod$p$ כאשר $y \in Q.R.(p)$ (y ידוע).

ב. הוכח כי הקבוצה - $S_2 = \{x \mid \left(\frac{x}{n}\right) = 1\}$ כש-$n=pq$ (p ו-q מס' ראשוניים גדולים לא ידועים) נשמרת תחת הצפנת RSA, עם מפתח (n,e) כש-$e \in Z^*_{\varphi(n)}$.

ג. הוכח כי הקבוצה $S_3 = \{x \mid x \in Q.R.(n)\}$, עבור n כמו בסעיף הקודם, נשמרת תחת הצפנת RSA, עם מפתח (n,e) כש-$e \in Z^*_{\varphi(n)}$.

ד. לכל אחת מן הקבוצות הנ"ל קבע אם היא נשמרת בולטת. אם כן, הצג את האלגוריתם המזהה את הקבוצה, ואם לא, נמק מדוע.

שאלה 4 (25 נק')

שאלה זו דנה בשתוף סוד.
נגדיר מטריצה M_3 להיות המטריצה הבאה

$$M_3 = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

כמו כן נגדיר את השלשה (y_1, y_2, y_3) להיות:

$$\begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$$

א. הראה כי אם x_1, x_2 נבחרים אקראית, x_3 הינו הסוד ו- (y_1, y_2, y_3) מחולקים כשלושה שתפים, אזי המערכת הנ"ל מגדירה סכמת סף (3,3).

ב. כדי להפוך את הסכמה ל-(n,n), הוחלפה M_3 ב- M_n

$$M_n = \begin{pmatrix} 2 & 1 & 1 & 1 \\ 1 & \ddots & 1 & 1 \\ 1 & 1 & 2 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}, \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} = M_n \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$$

כלומר M_n היא כולה 1-ים מלבד *n-1* האיברים הראשונים באלכסון שהם 2.
הראה שאם $x_1, \ldots, x_{n-1}$ נבחרים אקראית ו- x_n הינו הסוד, ו- $(y_1, \ldots, y_n)$ מחולקים כ-*n* שתפים, אזי המערכת הנ"ל מגדירה סכמת סף *(n,n)*.

ג. כדי להפוך את המערכת מסעיף א' לסכמת סף (2,3), הוחלט לחשב את x_2 ע"י $x_2 = 3x_1$ (במקום לבחור אותו באקראי). הראה שעבור בחירה שכזו מתקבלת סכמת סף (2,3).