מבוא לקריפטוגרפיה - תרגיל בית 1

נא להגיש עד ה 19.12.2016 דרך המודל. ההגשה היא ביחידים. התייעצות מותרת, אך חובה לרשום את הפתרונות לבד.

סודיות של מערכות הצפנה, ומושגים מתמטיים שימושיים בהקשר זה

1. בהרצאה טענו שהגדרה 2 והגדרה 3 לסודיות מושלמת של מערכת הצפנה הן שקולות. הראינו שאם מערכת הצפנה $E = (\text{Gen},\text{Enc},\text{Dec})$ מקיימת את הגדרה 3, אז היא מקיימת גם את הגדרה 2. הראו שהכוון ההפוך גם מתקיים. כלומר, אם E מקיימת את הגדרה 2, אז היא מקיימת את הגדרה 3.

2. עבור זוג מספרים שלמים $0 < l < t$ נגדיר צופן $(t,l) - Vigenere$ כמערכת הצפנה המוגדרת ע"י:

   - $\mathcal{M} = \mathcal{C} = \mathbb{Z}_{26}^t, \mathcal{K} = \mathbb{Z}_{26}^l$
   - האלגוריתם Gen מחזיר מחרוזת אקראית $k \in \mathbb{Z}_{26}^l$.
   - האלגוריתם $\text{Enc}(k,m)$ מחזיר $c = (c_1, \ldots, c_t)$ כאשר לכל i $c_i = m_i + k_{i \bmod l}$ כאשר החיבור מתבצע ב $\mathbb{Z}_n$.
   - אלגוריתם הפענוח $\text{Dec}(k,c)$ מחזיר $m' = (m'_1, \ldots, m'_t)$ כאשר לכל i $m'_i = c_i - k_{i \bmod l}$.

   הוכיחו כי צופן (t,l)-Vigenere אינו מקיים בטיחות מושלמת. לשם כך ניתן להשתמש בכל אחת מ 3 ההגדרות לבטיחות מושלמת. הגדרה 2 עשויה להיות הכי פשוטה לצורך העניין.

3.

   א. יהיו $g_1(n), g_2(n) : \mathbb{N} \to \mathbb{R}^+$ פונקציות זניחות. הוכיחו (במדוייק, מההגדרה) כי הפונקציה $f(n) = g_1(n) + g_2(n)$ גם היא זניחה.

   ב. השתמשו בסעיף הקודם, והוכיחו שלכל t פונקציות זניחות $g_1, g_2, \ldots, g_t$, $f(n) = \sum_{i=1}^{t} g_i(n)$ גם זניחה. ניתן להוכיח זאת באינדוקציה פשוטה על t.

   ג. הוכח שסכום של $t(n)$ פונקציות זניחות יכול להיות פונקציה שאינה זניחה (כאן t אינו מספר קבוע, אלא פונקציה של n). הסבירו בקצרה מדוע ההוכחה מהסעיף הקודם אכן אינה עובדת למספר לא קבוע של פונקציות.

   ד. הוכח או הפרך: אם g אינה פונקציה זניחה, אזי קיים פולינום $p(n)$ ומספר n_0 כך שלכל

$n > n_0$ מתקיים $g(n) \geq 1/p(n)$.

אלגוריתמים הסתברותיים

כזכור, אלגוריתם הסתברותי הוא אלגוריתם שמקבל מחרוזת אקראית r כפלט נוסף, ומתייחס לזוג x, y בתור קלט (פרט לכך, ניתן לחשוב עליו כאלגוריתם דטרמיניסטי "רגיל"). על מנת לדייק, נאמר ש r, x שייכות ל Σ^* כאשר Σ הוא א"ב הקלט.

בקריפטוגרפיה, משתמשים באקראיות על מנת להתגבר על תוקף אדוורסריאלי (כלומר, כזה שמנסה לפגוע בתהליך החישוב של המשתמשים החוקיים. למשל, ללמוד מידע על ההודעות המוצפנות). אינטואיטיבית, האקראיות, שידועה (לאחד או יותר) מהמשתמשים החוקיים ואינה ידועה לתוקף היא המפתח לבטיחות נגד התוקף.

בהקשר של אלגוריתמים, המטרה של שימוש באקראיות היא שונה בד"כ. מטרתה לאפשר לבנות אלגוריתם שרץ יותר מהר מאלגוריתמים דטרמיניסטיים, בתמורה לכך שמאפשרים טעות קטנה בתשובת האלגוריתם (הטעות היא קטנה לכל קלט שהוא). נראה כאן מספר דוגמאות.

1. נתון מערך a באורך $2n$ של 0-ים ו 1-ים. בדיוק מחצית מערכי המערך הם 0. עלינו למצוא זוג אידקסים במערך $i \neq j$ כך ש $a[i] \neq a[j]$ תוך ביצוע מספר מינימלי של גישות למערך (לא מעניין אותנו כאן זמן ריצה או גישות לזכרון נוסף שאינו המערך a - חישבו על המערך כמוסד נתונים רחוק, שהגישות אליו לוקחות הרבה זמן).

   א. בנה אלגוריתם דטרמיניסטי (שתמיד צודק) לפתרון הבעיה. מה מספר הגישות המקסילמלי למערך שהאלגוריתם מבצע?
   ב. הוכיחו כי לכל אלגוריתם דטרמיניסטי קיים קלט עבורו מספר הגישות למערך במקרה הגרוע הוא לפחות כמו של האלגוריתם בסעיף א'.
   ג. בנו אלגוריתם הסתברותי המבצע $O(\log^{1.1}(n))$ גישות למערך והסברות שגיאה זניחה ב n. (החזקה 1.1 היא שרירותית, כל מספר קבוע גדול מ 1 ייתן הסתברות שגיאה זניחה).

2. בשאלה זו ננתח אלגוריתם הסתברותי יעיל לבדיקת ראשוניות. האלגוריתם פותח ע"י Miller ו Rabin ב 1980, והוא האלגוריתם הראשון שעובד נכון (פרט לטעות קטנה) לכל קלט.
אלגוריתם זה הוא הכללה של הרעיון שאם n ראשוני אז $a^{n-1} = 1$ מודולו n לכל a (משפט פרמה הקטן). לשמחתינו, אם n פריק, הבדיקה עובדת לא רע, אך לא תמיד.

   א. בשאלה זו נפתח את אלגוריתם MR (לא להיבהל, רב העבודה הקשה תעשה כאן בשבילכם :). המשפט הבא הוא נכון (ללא הוכחה, אתם מוזמנים לחפש את ההוכחה באינטרנט ולהבין אותה. זה בהחלט אפשרי עם רקע מסויים בתורת המספרים).

   משפט: יהי $n > 2$ מספר אי זוגי. נסמן $n - 1 = 2^r \cdot d$ כאשר d מספר אי זוגי. אזי, אם n ראשוני, מתקיים לכל a בקבוצה $A = \{a | 0 < a < n, gcd(a, n) = 1\}$

   $(*) a^{n-1} = 1 \bmod n \text{ or } a^{2^r d} = -1 \bmod n \text{ for some } 0 \leq r < s$.

   יתרה מזאת, אם n אינו ראשוני, אז לפחות $3/4$ מהאיברים בקבוצה A אינם מקיימים את התנאי (*) לעיל. בנה אלגוריתם הסתברותי לבדיקת ראשוניות על סמך המשפט, הטועה בהסתברות $O(2^{-n})$.

ב. מה סבוכיות זמן הריצה של האלגוריתם מהסעיף הקודם (כאן נמדוד זמן ריצה במספר פעולות כפל וחיבור מודולו n)? השוו לסבוכיות האלגוריתם הדטרמיניסטי הנאיבי המחפש מחלקים עד השרש.