מבוא לקריפטולוגיה - דף תרגילים מספר 2

הנושא: צופני זרם

1. (20%) כיתבו תוכנית לפיענוח ciphertext שהוצפן באמצעות PRG לפי שיטת Blum Blum Shub. השתמשו בה לפענוח הקבצים הנתונים. בכל הקבצים המוצפנים הסיסמה היא שם הקובץ (ללא הסיומת bbs.).

2. (30%) נניח ש $G:\{0,1\}^s \to \{0,1\}^n$ הוא PRG בטוח. לכל אחד מהבאים יש לקבוע האם הוא PRG בטוח ולנמק (אם אין תשובה חד משמעית, הסבירו למה):
   א. $G':\{0,1\}^s \to \{0,1\}^n, \quad G'(k) = G(k \oplus 1^s)$
   ב. $G':\{0,1\}^s \to \{0,1\}^n, \quad G'(k) = G(k) \oplus 1^n$
   ג. $G':\{0,1\}^s \to \{0,1\}^{n-1}, \quad G'(k) = G(k)[0,\ldots,n-2]$
   ד. $G':\{0,1\}^s \to \{0,1\}^{2n}, \quad G'(k) = G(k) \| G(k)$ (|| הוא שרשור)
   ה. $G':\{0,1\}^s \to \{0,1\}^{2n}, \quad G'(k) = G(k) \| G(k)'$ ($G(k)'$ מתקבל מהיפוך הביטים ב $G(k)$)
   ו. $G':\{0,1\}^s \to \{0,1\}^{2n}, \quad G'(k) = G(k) \| G(k')$ (k' מתקבל מהיפוך הביטים ב k)
   ז. $G':\{0,1\}^{2s} \to \{0,1\}^n, \quad G'(k_1 \| k_2) = G(k_1) \wedge G(k_2)$, כאשר $\wedge$ מסמן bitwise and

3. (20%) נגדיר PRG באופן הבא: $G:\{0,1\}^4 \to \{0,1\}^{16}$, $G(k) = k \| ls(k) \| ls(k)^{(2)} \| ls(k)^{(3)}$ (ר' תרגיל 4). נגדיר מבחן סטטיסטי A כך ש $A(x)=1$ אם ורק אם x_6 לא מכיל רצף של 3 1-ים ולא מכיל רצף של 3 0-ים, כאשר x_6 היא המחרוזת המורכבת מ 3 הביטים הגבוהים ביותר ב- x ו-3 הביטים הנמוכים ביותר ב x. חשבו את $\mathrm{Adv}_{\mathrm{PRG}}[A,G]$.

4. (30%) יהי (E,D) צופן על (M,C,K), כך ש $K=\{0,1\}^\ell$ (אין צורך לדעת מיהם M ו – C). נניח שרוצים לחלק מפתח $k \in K$ בין שני אנשים, כך שרק אם שניהם חוברים יחד ניתן לדעת את המפתח k. ניתן לעשות זאת באופן הבא: בוחרים באופן אקראי מחרוזת $k_1 \in \{0,1\}^\ell$ ומחשבים את $k_2 = k_1 \oplus k$. נותנים לאחד האנשים את k_1 ולשני את k_2.
   א) הראו שאם שני האנשים חוברים יחד, אז הם יודעים את המפתח k, אבל כל אחד מהם לחוד לא יודע כלום אודות המפתח k.
   ב) עכשיו רוצים לחלק את המפתח k בין שלושה אנשים p_1, p_2, p_3 כך שכל שניים מהם יוכלו לדעת את k, אבל לאף אחד מהם לבד אין שום מידע על המפתח. לשם כך מייצרים שתי מחרוזות בינאריות $k_1, k_2 \in \{0,1\}^\ell$ ומחשבים את $k_1' = k_1 \oplus k$ ו $k_2' = k_2 \oplus k$. איך צריך לחלק את המחרוזות הנ"ל בין p_1, p_2, p_3 כדי להשיג את המטרה? (רמז: ניתן לתת לאדם יותר ממחרוזת אחת)

יש להגיש שני קבצים במוודל:
1) קובץ py ובו פתרון שאלה 1.
2) קובץ pdf ובו פתרון שאלות 2,3,4