יש לפתור **ארבע** מחמש השאלות.

שאלה 1 (25 נקודות)

נרצה לממש פעולה נוספת על ערימות בינומיות: Binomial_Heap_Split(H) מקבלת כקלט ערימה בינומית H שבה n איברים ומפצלת אותה לשתי ערימות בינומיות H_1 ו- H_2 כך שב- H_1 יש $\left\lfloor \frac{n}{2} \right\rfloor$ איברים וב- H_2 יש $\left\lceil \frac{n}{2} \right\rceil$ איברים.

הצע מימוש יעיל לפעולה זו. הסבר את נכונותו ונתח את סיבוכיותו.

שאלה 2 (25 נקודות)

נתאר אפליקציה של שיטת הצפנה שהוצעה ע"י Pohlig ו- Hellman לשני משתמשים:

יהי p ראשוני גדול הידוע לכולם. כל משתתף i בוחר באקראי e_i הזר ל- $(p-1)$, מחשב את ההפכי שלו d_i, מודולו $(p-1)$ (כלומר: $e_i \cdot d_i \equiv 1 \bmod (p-1)$) **ושומר את שניהם בסוד.**

כאשר A רוצה לשלוח הודעה M, $0 < M < p$ אל B, הם מבצעים את הפרוטוקול הבא (כל החישובים מתבצעים מודולו p):

א. A שולח אל B את M^{e_A}

ב. B שולח אל A את $(M^{e_A})^{e_B} \equiv M^{e_A \cdot e_B}$

ג. A שולח אל B את $(M^{e_A \cdot e_B})^{d_A} \equiv M^{e_B}$

ד. B מחשב את $(M^{e_B})^{d_B} = M$

האם אפליקציה זו היתה נכונה אם במקום לבצע הצפנה של M ע"י M^{e_i} ופענוח הודעה מוצפנת C ע"י C^{d_i} היו משתמשים בשיטת הצפנה כלשהי $(E(M), D(C))$ המקיימת $D(E(M)) = M$? אם כן, הסבר איך. אם לא, הסבר איזו תכונה בשיטת ההצפנה הזאת מאפשרת שימוש באפליקציה זו והראה דוגמה לשיטת הצפנה שבה אפליקציה זו לא תעבוד (לצורך כך, אינך צריך להתייחס לבטיחותה של שיטת ההצפנה שאתה מציע; די שתראה זוג אופרטורים כלשהם $(E(M), D(C))$ המקיימים $D(E(M)) = M$ עבורם האפליקציה שלעיל לא תעבוד).

שאלה 3 (25 נקודות)

א. האם עבור כל n טבעי וזוגי אפשר להגיע, ע"י הפעולות המותרות על ערימת פיבונצ'י, לערימת פיבונצ'י המכילה n צמתים, ומורכבת רק מאוסף של עצים בינומיים לא סדורים U_k (כלומר, רק עצים כאלה: ). אם כן - הראה כיצד. אם לא - הוכח.

ב. האם עבור כל m טבעי אפשר להגיע, ע"י הפעולות המותרות על ערימת פיבונצ'י, לערימת פיבונצ'י המכילה m עצים, כאשר העץ ה- i מכיל i צמתים? אם כן - הראה כיצד. אם לא - הוכח.

שאלה 4 (25 נקודות)

הוכח או הפרך את הטענה הבאה:

בהנתן רשת מיון ל- n קלטים (הנח כי n חזקה של 2 ו- $4 \le n$) אם ניקח תת קבוצה כלשהי של תיילי קלט בגודל $\frac{n}{2}$, ונמחק מהרשת את כל התיילים האחרים ואת כל המשווים שמתייחסים לתיילים האחרים (או להמשכם, בעומק כלשהו של הרשת) נקבל רשת מיון עבור $\frac{n}{2}$ תיילי הקלט הנשארים.

שאלה 5 (25 נקודות)

בהינתן תבנית P, תאר כיצד בונים אוטומט סופי המוצא בטקסט נתון את כל המופעים של P שההיסט שלהם הוא זוגי.

למשל, אם P היא התבנית $abba$ והטקסט הוא $abbabbabba$ אז המופעים המתאימים נמצאים בהיסטים 0 ו-6. גם בהיסט 3 יש מופע של P אך זהו היסט אי-זוגי.

סוף!