יש לפתור ארבע מחמש השאלות.

שאלה 1

בבניית מערכת RSA בוחרים $n = p \cdot q$ ו- e באקראי כך ש- $\gcd(e, \phi(n)) = 1$. הערך d מחושב להיות ההפכי של e מודולו $\phi(n)$, כלומר $e \cdot d \equiv 1 \pmod{\phi(n)}$ התייחס להצעה הבאה:

$\mathrm{lcm}(a, b)$ היא הכפולה המשותפת המינימלית של a, b, כלומר, השלם האי-שלילי הקטן ביותר שהוא כפולה של a וכפולה של b. יהי $\psi(n) = \mathrm{lcm}((p-1), (q-1))$.

נבחר באקראי e מבין כל המספרים המקיימים $\gcd(e, \psi(n)) = 1$ ונחשב את d להיות ההפכי של e מודולו $\psi(n)$. כלומר $e \cdot d \equiv 1 \pmod{\psi(n)}$.

האם תכונות מערכת ה- RSA (הצפנה ופענוח) נשמרות במקרה כזה? הוכח.

שאלה 2

ברצוננו להרחיב את מבנה הנתוניב של ערימה בינומית כך שיתמוך בפעולה חדשה:

BINOMIAL_HEAP_INCREASE_KEY(H, k, x) אשר מגדילה את ערכו של המפתח של הצומת x בערימה H לערך k. הצג מימוש יעיל של הפעולה ונתח את סבוכיותו.

שאלה 3

נניח שבמקום משווה של שני תילי קלט ושני תילי פלט נתון לנו משווה של ארבעה תילי קלט וארבעה תילי פלט. בארבעת תילי הפלט של המשווה יופיעו ארבעת ערכי הקלט כאשר הם ממויינים מקטן לגדול - הקטן ביותר בתיל העליון והגדול ביותר בתיל התחתון.

עוד נניח שבבניית רשת מיון הנעזרת ברשת מיזוג, הרשת (כולל רשת המיזוג) יכולה להכיל רק משווים כאלה ולא משווים רגילים. (הנח כי n - מספר תילי הקלט ברשת - הוא חזקה של 2 ו- $n \geq 4$).

א. הראה כיצד תראה הרשת המתקבלת.

ב. מה יהיה עומקה של הרשת?

ג. כמה משווים מכילה הרשת?

שאלה 4

בהנתן תבנית P , הראה כיצד בונים אוטומט סופי המוצא בטקסט את כל זוגות המופעים של P המופרדים ע"י שני תוים כלשהם.

למשל, כאשר T הוא הטקסט abcaabcababcbbaabcabc ו- P היא התבנית abc, רק היסט $s = 4$ הוא היסט תקף עבור שאלה זו כי $T[5..12] = abcababc$ המכיל בדיוק שני מופעים של P המופרדים ע"י שני תווים (ab), ואין אחרים כאלה.

שאלה 5

בערימת פיבונצ'י אנו מעוניינים לתמוך גם בפעולה שמחזירה את האיבר הקטן ביותר בערימה פרט לאיבר המינימלי SECOND_MIN, כך שעלותה תהיה $\theta(1)$ (במקרה הגרוע). המבנה החדש צריך גם לתמוך בכל הפעולות הקיימות, ללא שינוי בעלותן.

תאר איזה שינויים עליך לבצע במבנה הנתונים, ובפעולות הקיימות, וכיצד תממש את הפעולה החדשה.

סוף!