מבוא לקריפטולוגיה - דף תרגילים מספר 3

1. (30%) בתוכנית זו עליכם להתשמש בנוסחה לחישוב פונקציית אוילר מההרצאה
   א. כיתבו תוכנית בפייתון שקוראת מספרים מקובץ numbers.txt (מצורף) ומחשבת את פונקציית אוילר שלהם.
   ב. עכשיו כיתבו תוכנית חדשה שמייצרת מספרים אקראיים, באמצעות הפונקציה urandom, בגודל 12 בתים כל אחד (שזה הגודל הממוצע של המספרים בקובץ numbers.txt) ומחשבת את פונקציית אוילר שלהם. הריצו את התוכנית.
   ג. הסבירו מדוע התוכנית נותנת תוצאה בסעיף א' בזמן סביר אבל לא נותנת תוצאה בסעיף ב'.

2. (30%) (עפ"י Ellis) להלן סכמת הצפנה שבה Bob מצפין ידיעה עבור Alice:
   i. Alice בוחרת שני ראשוניים שונים P ו Q, כך ש P זר ל Q–1 ו Q זר ל P–1.
   ii. Alice מפרסמת את N=PQ.
   iii. Alice מחשבת את P' ו Q' כך ש $PP' \equiv 1 \pmod{Q-1}$ ו $QQ' \equiv 1 \pmod{P-1}$
   iv. Bob מצפין ידיעה M באופן הבא: $C = M^N \pmod N$
   v. Alice מוצאת את M ע"י חישוב $0 \le M' < N$, כך ש...
   $M' \equiv C^{P'} \pmod Q$ ו $M' \equiv C^{Q'} \pmod P$ בעזרת משפט השארית הסיני

   א. הראו שסכמה זאת עובדת, כלומר M'=M. (רמז: משפט השארית הסיני)
   ב. מה ההבדל ומה המשותף בין סכמה זאת לבין RSA?
   ג. מה היתרונות שיש ל RSA על-פני סכמה זאת?

3. (40%) עבור מספר n אי-זוגי <u>שאינו ראשוני</u> נגדיר PS(n) כמספר הבסיסים a שעבורם n הוא ראשוני מדומה חזק (כלומר, מבחן מילר רבין מגדיר את n כראשוני). בכתה ראינו ש $PS(n)/(n-1) < 1/4$. כמו-כן, נגדיר PS*(n) כמספר הבסיסים a שעבורם n מוגדר כראשוני לפי מבחן Lehmann. ידוע ש $PS^*(n)/(n-1) < 1/2$.
   כתבו תוכנית מחשב שמחשבת את PS(n)/(n-1) ואת PS*(n)/(n-1) עבור כל המספרים האי-זוגיים <u>הלא-ראשוניים</u> בין 1,000,000 ל 2,000,000.
   פלט התוכנית:
   1) הערך המקסימלי של PS(n)/(n-1) עבור n-ים לא ראשוניים.
   2) הערך הממוצע של PS(n)/(n-1) עבור n-ים לא ראשוניים.
   3) הערך המקסימלי של PS*(n)/(n-1) עבור n-ים לא ראשוניים.
   4) הערך הממוצע של PS*(n)/(n-1) עבור n-ים לא ראשוניים.
   5) מספר ה n-ים שעבורם PS*(n)/(n-1) < PS(n)/(n-1)
   6) מספר ה n-ים שעבורם PS*(n)/(n-1) > PS(n)/(n-1)
   7) מספר ה n-ים שעבורם PS*(n)/(n-1) = PS(n)/(n-1)

הנחיות הגשה:

1) יש להגיש בקובץ PDF:
- ערכי $\phi(n)$ של המספרים בסעיף א' של שאלה 1
- סעיף ב' של שאלה 1
- שאלה 2
- פלט התוכנית בשאלה 3

2) יש להגיש בנפרד את התוכניות של סעיפים א' ו-ב' של שאלה 1 ואת התוכנית בשאלה 3.