

תרגיל 12

שאלה 1. בוב מעוניין לשלוח לאליס הודעה באופן מוצפן. ולכן, אליס בוחרת שני מספרים ראשוניים. $p=13$, $q=23$. בנוסף, אליס בוחרת את המספר $e=35$.
א. הראה ש- e הנ"ל אכן בחירה תקינה.
ב. חשב את d (המקיים $de \equiv 1 \pmod{\phi(n)}$ כאשר $n = p * q$)
ג. אליס שולחת לבוב את n ואת e וכעת הוא יכול להצפין. בוב מעוניין להצפין את ההודעה $m=15$. נשים לב כי ההודעה m אכן עומדת בקרטיונים. חשבו את ההודעה אותה בוב יעביר לאליס.
ד. הראו כי אליס אכן יכולה לפענח את ההודעה.

שאלה 2. א. חשב FFT של הסדרה הבאה: $[2\ 2\ 6\ 9]$.

ב. חשב FFT של הסדרה הבאה: $[2\ 2\ 6\ 9\ 2\ 2\ 6\ 9]$.

ג. בהינתן הסדרה $0\ 0\ 0\ 0\ 1\ 1\ 1\ 1$ איך יראה סדר הנתונים לאחר bit-reversal.