תרגיל 12 פתרון

88-280 סמסטר א' תשע"ח

תרגיל 2. א. לאחר החישוב יתקבל [38 -8+14i -6 -8-14i]

ב[38 0 -8+14i 0 -6 0 -8-14i 0]

ג. לאחר ה*bit-reversal* סדר הנתונים הוא *0 1 0 1 0 1 0 1* . וודאו שאתם יודעים כיצד להראות זאת. (הראנו זאת בתרגול האחרון).

תרגיל 1.

4.א. נראה ש $\gcd(\varphi(n),e)=1$,n=p*q.

q,p ראשוניים ולכן $\varphi(n)$ =(p-1)*(q-1)=264

נראה בעזרת אלגוריתם אוקלידס:

gcd(264,35)=[264=7*35+19]

gcd(35,19)=[35=19*1+16]

gcd(19,16)=[19=1*16+3]

gcd(16,3)=[16=5*3+1]

gcd(3,1)=1

=>gcd(264,35)=1

ב.נרצה למצוא את ההופכי של e מודלו $\varphi(n)$.ניעזר בפירוק שך סעיף א':

1=16-5*3

1=16-5(19-16*1)=6*16-5*19

1=6*(35-19*1)-5*19=6*35-11*19

1=6*35-11(264-7*35)=83*35-11*264

ולכן d=83

ג.בוב ירצה לשלוח את$c=m^e \bmod(n)$

$C=15^{35}mod299$

נעלה כאן בחזקה.

נגיע ש$c=189 \bmod 299$.

ד. נרצה לפענח את ההודעה. נחשב:

c=189

d=83

n=299

נרצה לחשב $m=c^d mod(n) = 189^{83} mod(299)$

נעלה את החזקות ונקבל $15 \bmod(299)$ ולכן אליס הצליחה לפענח את ההודעה.