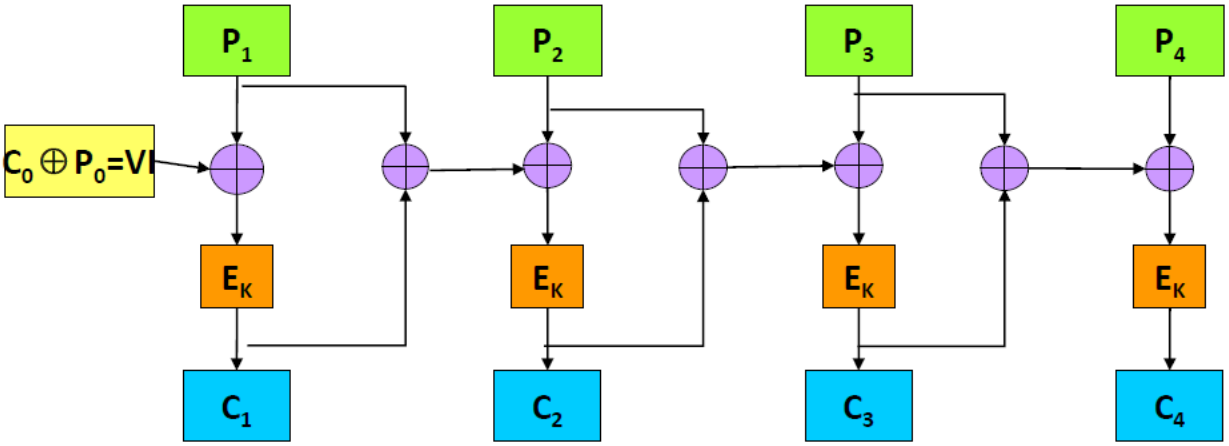
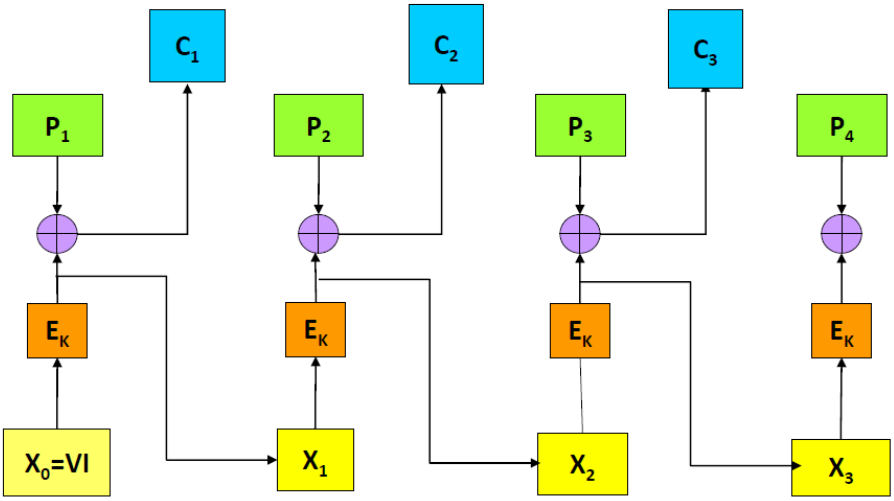
מבוא להצפנה: תרגיל 3

1. מוגדרים שיטות ההפעלה הבאות:

MOP1:



ו-MOP2:



עבור כל אחד מהשיטות האלה:

a. כתבו את פונקצית ההצפנה ופונקצית הפענוח.

b. נניח כי סיבית אחת של הבלוק C_2 מתחלפת בתקשורת. בברו את ההשפעה על פענוח ההודעה.

c. אליס שולחת הודעה לבוב בעזרת שיטת ההפעלה MOP2. אוסקר מיירט את ההודעה של אליס. הוא יודע שהבלוק השלישי הוא הכתובת לפגישה חשובה. אוסקר יודע את הכתובת ולכן הוא יודע את P_3 . הסבירו איך הוא יכול לשנות את ההודעה של אליס לפני שהוא מעביר אותה לבוב כך שבוב לא יקבל את הכתובת הנכונה.

2. עבור שיטות ההפעלה CBC ו-CFB: מה קורה אם בלוק שלם (נגיד C_3) נמחק בזמן העברת ההודעה?

3. ניתן גם להגדיר את שיטות ההפעלה CBC עבור צופני בלוקים העובדים עם אותיות במקום סיביות אם מחליפים את ה-XOR בסכום מודולו $\mathbb{Z}_{26}$. הצפינו את ההודעה TESTOFMETHOD לפי השיטה הזו עם בלוק התחלתי INIT עבור צופן היל עם מפתח $\begin{pmatrix} 3 & 4 & 2 & 1 \\ 3 & 2 & 3 & 4 \\ 1 & 5 & 2 & 3 \\ 4 & 1 & 2 & 1 \end{pmatrix}$.

4. מפתח של צופן LFSR מאורך 5 מוגדר על ידי הערכים התחלתיים: 10011 ונוסחת הנסיגה $x_{n+5} = x_{n+1} \oplus x_{n+2} \oplus x_{n+3}$.

   a. מצאו את אורך המחזור של סדרת הסיביות של המפתח.

   b. השתמשו במפתח כדי להצפין את ההודעה 00111 00101 01010 10110 .

   c. מצאו נוסחת נסיגה באורך מינימלי היוצרת אותו מפתח.

5. בחרו שני ראשוניים p,q מתוך $\{101,103,107,109,113,127,131,137,139\}$ ויהי $n = pq$. בחרו e כך ש-(n,e) הוא מפתח ציבורי ל-RSA וחשבו את המפתח הפרטי בעזרת האלגוריתם האוקלידי המורחב שהוצג בשיעור.. הראו את החישובים.

בהצלחה!