3.a) FMS מחפש פקטות אשר מתחילות בצורה ידוע של

1st byte: v1=3, v2=255, v3=x

2nd byte: v1=4, v2=255, v3=x

על כול פקטה מריצים KSA כמספר הביט שרוצים למצוא במפתח + 1, מריצים את האלגוריתמים על כמה שיותר פקטות שעומדות בתנאי התחלה. לאחר כול ריצה של האלגוריתמים מקבלים ביט שיש סיכוי שהוא הביטי הנכון של מפתח. לאחר ריצה על מספר פקטות מגבלים את מצב הביט בעל הסיכוי הגבוה ביותר שהוא נכון.

ההתקפה עובדת משום שהפקטות לא באמת רנדומליות אלה יש להם תפוס חוזר כול כמה פקטות בצורה קבוע.

סיסמה לtraffic1: ro@!1