**מבוא להצפנה – תרגיל 1**

* *GE ----> IS*

*ז"א: e(6) = 8; e(4) = 18*

* *EG ----> IS*

*ז"א: e(4) = 8; e(6) = 18*

*האות הנפוצה ביותר בצופן הראשון (M1) היא: k*

*האות הנפוצה ביותר בצופן השני (M2) היא: a*

נניח כי האות הנפוצה ביותר במקור היא o :

* *M1: אם o מוצפן ל- k אז זאת הזזה של והפענוח נותן:*

*b o b s u h x q x o q y h k u f o g d e t q o h k x o u t y i w*

*ולהודעה זאת אין משמעות.*

* *M2: אם o מוצפן ל- a אז זאת הזזה של והפענוח נותן:*

*b o b w a n t s t o s i n g a j o y f u l s o n g t o a l i c e*

*קיבלנו הודעה עם משמעות:*

*bob wants to sing a joyful song to alice*

*מצאנו כי ההודעה M2 מוצפנת עם צופן הזזה:*

*והעתקת הפענוח היא:*

*ההודעה M1 מוצפנת על ידי צופן אפיני. נשתמש בשתי אותיות של הצופן וטקסט מקור כדי למצוא את העתקת ההצפנה וההעתקת הפענוח.*

האות a=0 מוצפנת כ- q=16. ולכן

האות b=1 מוצפנת כ- x=23*. ולכן*

*פונקציית ההצפנה היא:*

*פונקציית הפענוח היא:*

האות a=0 מוצפנת כ- q=16. ולכן

האות b=1 מוצפנת כ- x=23*. ולכן*

*פונקציית הפענוח היא:*

*מספר הפתרונות של המשוואה הזו הוא או 0 או gcd(a-1, 30) .*

1. *, לכן לכל a לא מתקיים ש- gcd(a-1, 30) = 7 .*

*לא קיימים a ו- b כך שמספר הפתרונות ל- הוא 7.*

1. *, לכן קיים a כך ש- 6 gcd(a-1, 30) = ( צריך להיות שווה ל- 6).*

*נבחר- , .*

*ניתן דוגמא:*

*יהיו לנו 6 פתרונות כאשר: 6 = gcd(a-1, 30) ו- (-b)|6.*

*למשל - .*

*קיים צופן אפיני לכל x אם (a+1) הוא מספר הפיך. ואז מתקבל:*

*למשוואה יש 28 פתרונות לכל X אם מתקיים ש- 28 = gcd(a-1, 28) וגם מתקיים: .*