# תרגיל בית 2

## מגיש: יהונתן לוסקי, 315690677

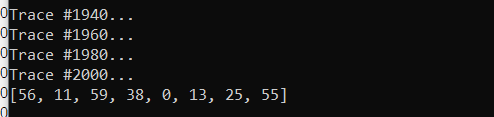
## CPA Attack:

בסעיף זה הרצתי את התוכנית שניתנה באמצעות matlab והבנתי מה היא עושה. לאחר מכן תירגמתי את התוכנית ל-python תוך שימוש בספריות scipy, matplotlib ו-numpy. התוכנית מבצעת התקפה זהה לזאת של ה-matlab ועובדת על אותן הטבלאות.

התיעוד של התוכנית קיים בתוך קובץ ה-python המצורף. כמו כן, התכנית נכתבה עבור python 2.7.

## DPA Attack:

תחילה הרצתי את ההתקפה יחד עם כל ה-2000 traces. התוצאה שקיבלתי הינה המפתח הבא (למעשה אותו מפתח שהופיע גם באתר שהכיל את כל הקוד והמידע):



לאחר מכן, הרצתי את התוכנית עם 10,20,50 ו-100 traces ואחרי זה בקפיצות של 100 traces כל פעם, עד אשר התוצאות התייצבו. להלן התוצאות:

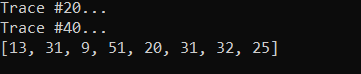
**10:**



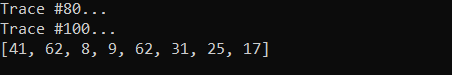
**20:**



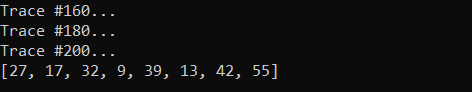
**50:**



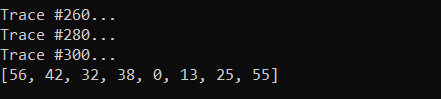
**100:**



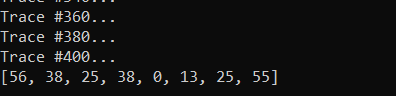
**200:**



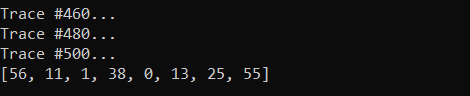
**300:**



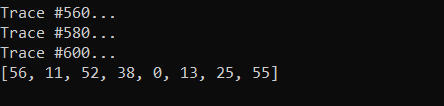
**400:**



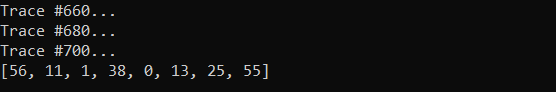
**500:**



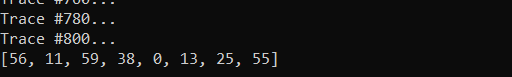
**600:**



**700:**



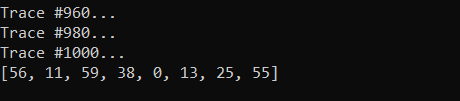
**800:**



**900:**



**1000:**



קל לראות שהתוצאות התייצבו סביב ה-800 traces כאשר קיבלנו את כל 8 הבתים הנכונים. מעניין לציין כי כבר סביב ה-300 traces כבר קיבלנו 6 בתים נכונים מתוך 8.