**תרגיל בית 3 בהנדסה לאחור**

**Hooking**

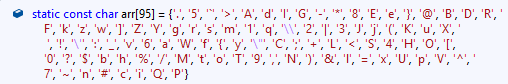
**דרור כרמון 036861292**

**עידו מנגר 212324313**

**חלק יבש**

**חלק רטוב**

**השבת השודד – חלק ראשון – ניתוח דינמי**

התחלנו בניתוח סטאטי של keygen.exe וראינו שהתוכנית מקבלת ארגומנט יחיד (key), מעתיקה רצף של בתים אל המחסנית ולאחר מכן מבצעת call לבית הראשון שהועתק אל המחסנית. המשמעות היא שהתוכנית עוברת לרוץ מקוד על המחסנית. כדי לראות את הקוד החל מקריאה זו עברנו לניתוח דינאמי בעזרת דיבאגר.  
הפונקציה שרצה מהמחסנית (נקראה לה keygen) מקבלת את key כפרמטר. מאתחלת ע"ג המחסנית מערך תווים (arr) בגודל 95. המערך נראה כך:

לאחר מכן הפונק' מקצה מקום לפלט (לפי גודל הקלט) ומתרגמת את הקלט בצורה הבאה:

1. len 🡨 strlen(key)
2. for i 🡨0 to len :
3. index 🡨 key[i] - ' '
4. output[i] 🡨 arr[index]

כתבנו את התוכנית keygen\_rev.exe אשר מבצעת את הפעולה ההפוכה.  
הרצנו אותה עם קלט סיסמת הגישה לאתר שקיבלנו בתרגיל הראשון **CMX3GBV11Q7R7OK9**  
וקיבלנו את סיסמת הגישה לדף הtools : **VgHB'/u==}w1w^Fk**

**השבת השודד – חלק שני hooking -**