**אבטחת מידע – תיאוריה בראי המציאות – תרגיל 1**

**PKCS-1.5**

תוקף יכול למדוד את הזמן שלוקח תהליך הפענוח. במהלך תהליך הפענוח אנו קוראים את כל הבתים של הצופן כדי למצוא את הבית שבו נגמר הpadding. משך זמן הריצה הוא ביחס לינארי ישן לגודל הpadding. ע"י ביצוע יוריסטיקות מתאימות נוכל להעריך את גודל הpadding על סמך משך זמן הפענוח ומכאן לגזור את אורך ההודעה המוצפנת (k-|pad|-3).