אבטחת מידע – תיאוריה בראי המציאות – תרגיל 1

SBS-HMAC

As the algorithm is structured, an attacker can derive the padding validity from the decryption's run time. Namely, they can derive if the padding is valid or not.

An attacker can derive a benchmark run time from a valid message (a message they encrypted and measured the run time of the decryption function) and use it to identify messages failing on padding validation (those will have a shorter run time). With that information at hand, the attacker can apply a padding oracle attack to decrypt the ciphertext blocks (except the first one), for example.

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).