Padding Oracle Attack

- איך מנפים כדי שקובץ הטקסט יתלקח מקובץ הבלוק-
העיקרי שיוסיף כמה בית של ניפוך יהיה כמות הבתים שמנפים.
לדוגמא "hello world" תופס 11 בתים אז יוסיף בסוף 5 בתים
בהם מוסיף 0X05.

- האורקל מהימן ciphertext תקבוד באופן הבא-
תבצע פענוח ותבדוק אם הפענוח תוקי. הפענוח יהיה תוקי במידה
וההריפוד תוקן.
במידה והריפוד תוקי- היו תחזיר את הפענוח. אחרת היו תרתיע שגיאה.
דוגמא לריפוד לא תוקי - הבא האותיון בפענוח הוא 4, אבל שלושה הבתים
לפניו הם לא 4.

- איך נבצע את ההתקפה? נשלח לאורקל את $x_j || c_i$ עבור c_i כלשהו.

① נתפש בלוק x_j שבאמצע שהאורקל יחזיר עבורו true (פענוח תוקי).
בכל פעם ניקח בית אחד (נתחיל מהאותיון) ונעבור מ מ מאופקי 00-ff עד
עד שיהיה מ שעבורו נקבל true.
הסיבה שלו היו שפענוח הבא האותיון יהיה 1 ובכך נקבל ריפוד תוקי ופענוח.

② נסמן את הפענוח כאור P'_2.
נשתמש בנוסחא שהגדנו בהרצאה שלה בחזרה-

$$P'_2[x] = P_i[x] \oplus C_{i-1}[x] \oplus x_j[x]$$

$$P_i[x] = P'_2[x] \oplus C_{i-1}[x] \oplus x_j[x]$$

נתון לנו נתון לנו הזלנו שלו נגא

③ לאחר מכן כדי לחבנו מ נוסף (בפעם האחרת לפני אחרון בבלוק) נבחר שלאחר פענוח
ב הרמוני בסוף יהיו 2 (ובכך הריפוד יהיה תוקי).
כלומר נרצה ש- $P'_2[x] = 0x02$ לכן נביא בחשבון המשוואה לעצלה ונבדוק מה
הבית של x_j בכך לפיה בבית האותיון כדי שפענוח יהיה שם 2.

④ את הבית הזה נקבל בעור הבית האותיון של x_j ונבדוק את שלב 1 שם
אך הפעם נשנה את הבית הלפני אחרון והבית האותיון יהיה מקובל.