# CSCI 3330: CBC Padding Oracle Exercise

In the following exercises assume the use of a 128-bit (16 byte) block cipher.

## 1 PKCS#7 padding warmup

The last block of my data before padding has only six bytes: [0,1,2,3,4,5]. What does the last block of my data look like when PKCS#7 padded?

Suppose now that the last block of my data before padding is

[0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15].

What does the last block of my data after padding look like?

### 1.1 Definitions for the remaining problems

Let $D(x)$ be the block cipher decryption of $x$, $C_i$ be the original $i$th ciphertext block, $C'_i$ be the modified $i$th ciphertext block, and $P_i$ be the $i$th plaintext block. Assume that all blocks are 16 bytes.

## 2 Determining valid padding byte

We try feeding all 256 possible values of $C'_{n-1}[15]$ (i.e., the last byte of $C'_{n-1}$) into our padding oracle. Only one value of $C'_{n-1}[15]$, $C'_{n-1}[15] = 0\text{xf0}$, results in valid padding. What is the value of the valid padding byte? Now write an equation for $D(C_n)[15]$ in terms of 0xf0 and the valid padding byte.

## 3 Inferring a byte of plaintext

Write an equation for $P_n[15]$ in terms of $D(C_n)[15]$ and $C_{n-1}[15]$. Suppose $C_{n-1}[15] = 0\text{x03}$. Plug in this value and your previous equation for $D(C_n)[15]$ to find $P_n[15]$.

## 4 Inferring another byte of plaintext

Now we want to infer $P_n[14]$. Before we repeat this attack by modifying $C'_{n-1}[14]$, what do we need to set $C'_{n-1}[15]$ to?