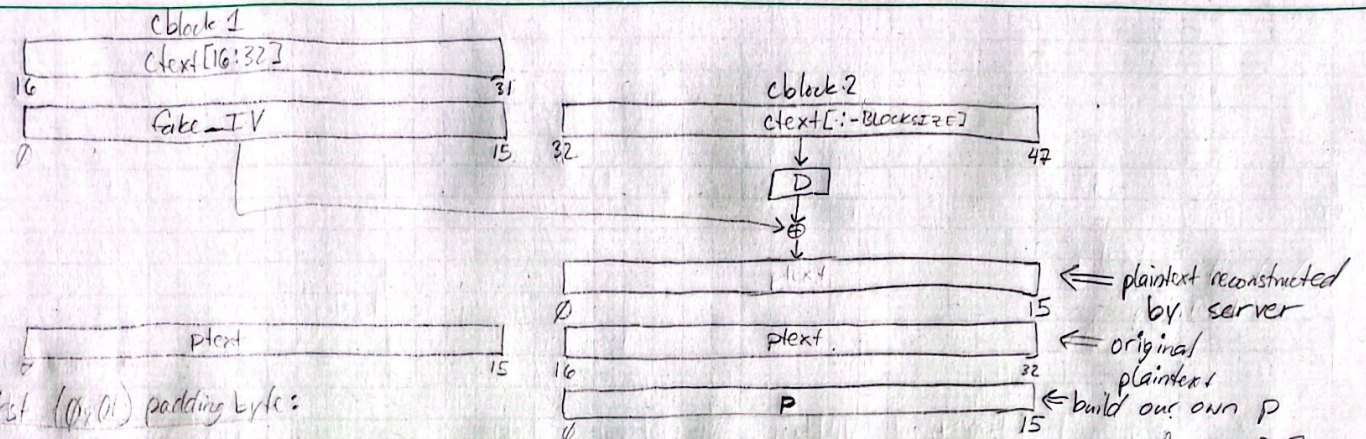


actual IV



For first (0x01) padding byte:

When padding valid, $\text{fake_IV}[15] \oplus \text{Decrypt}(\text{ciphertext}[47]) = 0x01 \Rightarrow \text{Decrypt}(\text{ciphertext}[47]) = \text{fake_IV}[15] \oplus 0x01$
 Since we know originally, $\text{ciphertext}[31] \oplus \text{Decrypt}(\text{ciphertext}[47]) = \text{plaintext}[31]$,
 we can now get $\text{plaintext}[31] = \text{ciphertext}[31] \oplus \text{fake_IV}[15] \oplus 0x01 \Rightarrow \text{set as } p[15]$

To set up ctext for next round (i.e. set last byte of ctext to 0x02):

We want $\text{fake_IV}[15] \oplus \text{Decrypt}(\text{ciphertext}[47]) = 0x02 \Rightarrow p[15] \oplus \text{fake_IV}[15] = \text{Decrypt}(\text{ciphertext}[47]) = \text{ciphertext}[31] \oplus \text{fake_IV}[15] \oplus 0x01 \oplus \text{fake_IV}[15]$
 $\Rightarrow \text{fake_IV}[15] \oplus (\text{ciphertext}[31] \oplus 0x01) = 0x02$
 $\Rightarrow \text{fake_IV}[15] = \text{ciphertext}[31] \oplus 0x01 \oplus 0x02$

For second (0x02) padding byte:

$$\text{plaintext}[30] = \text{ciphertext}[30] \oplus \text{fake_IV}[14] \oplus 0x02 \Rightarrow p[14]$$

General Rule (for 1 block of ctext attempting to pad w/ "target" # bytes): $p[16 - \text{target}] = \text{ciphertext}[16 - \text{target}] \oplus \text{fake_IV}[16 - \text{target}] \oplus \text{target}$

For prepping for 3rd round: We want $\text{fake_IV}[15] \oplus \text{Decrypt}(\text{ciphertext}[47]) = \text{fake_IV}[14] \oplus \text{Decrypt}(\text{ciphertext}[46]) = 0x03$
 right now: $\text{fake_IV}[15] \oplus \text{Decrypt}(\text{ciphertext}[47]) = 0x02 \Rightarrow \text{fake_IV}[15] = 0x02 \oplus 0x01 = 0x03$
 $\Rightarrow (\text{fake_IV} \oplus 0x02 \oplus 0x03) \oplus \text{Decrypt}(\text{ciphertext}[47]) = 0x02$
 $\Rightarrow \text{fake_IV}[15] \oplus \text{Decrypt}(\text{ciphertext}[47]) = 0x02 \oplus 0x02 \oplus 0x03 = 0x03$

General Rule: To prep for "target" padding, set $\text{fake_IV}[x] = \text{fake_IV}[x] \oplus (\text{target} - 1) \oplus \text{target}$