Segurança de Dados - Assignment 1

Pedro Malainho PG61005

1. Question 1

We know that both ciphertexts were produced with AES-OFB using the same key and IV. Because OFB with the same key/IV yields the same keystream, I recovered the keystream from the first pair and reused it to recover the second plaintext. Concretely: $P_1 \oplus C_1 = \text{Keystream}$.
And therefore since XOR is commutative, this is equivalent to get the plaintext on the second cipher like this, $C_2 \oplus \text{Keystream} = P_2$.

2. Question 2

Yes, AES-OFB can be broken if the IV and the key are reused. When the same key and IV are used, the initial keystream block (O_0) is identical for both plaintexts. This means that XORing the ciphertexts effectively gives us:

.

$$C_1 \oplus C_2 = (P_1 \oplus O_0) \oplus (P_2 \oplus O_0) = P_1 \oplus P_2$$

Even if neither plaintext is known initially, techniques such as crib-dragging (as demonstrated in code) or other cryptanalytic methods can be used to recover the original messages.