問4.2

解読対象の暗号文を(U, c), その平文をmとする。

$m_1 \in \mathbb{Z}_{|P|}$をとり、$c_1 := c \oplus m_1$を復号オラクルに聞く。

その出力m'は.

$$m' = u_x \oplus c_1$$
$$= u_x \oplus c \oplus m_1$$
$$= m \oplus m_1$$

となる。

$m = m' \oplus m_1$であるから. 解読できた。