問4.1

今、平文と暗号文の組 $(m_1, (U, c_1))$ が判明しているとする。

攻撃対象の暗号文を (U, c) とする。

乱数 r は共通であるから U は暗号にかかわらず等しく $U = (u_x, u_y)$ と表せる。

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

であるから、

$$c \oplus c_1 = (u_x \oplus m) \oplus (u_x \oplus m_1)$$

$$= m \oplus m_1$$

$\therefore m = c \oplus c_1 \oplus m_1$ であり、c, c_1, m_1 は既知であるから

解読できた。