

演習 4.1

既知の平文, 暗号文 m_1, U, c_1 は $m_1 = 3, U = (4, 0), c_1 = 7$ であり, 解読対象の暗号文は $U = (4, 0), c = 6$ である。

c に対応する平文を m とすると, 問 4.1 より,

$$\begin{aligned} m &= c_1 \oplus c \oplus m_1 \\ &= (111_2) \oplus (110_2) \oplus (011_2) \\ &= 2 \end{aligned}$$