Correction to exercise 4:

Part 1 of the exercise:

Recall that
$$P_M(m) = \begin{cases} p & \text{if } m=1 \\ 1-p & \text{if } m=0 \end{cases}$$

$$P_K(0) = P_K(1) = 1/2$$

and
$$C = M \oplus K.$$

Question 1:

The random variable C is an XOR between two binary variable, hence, it is a binary random variable
$$C \in \{0, 1\}.$$

Question 2:

Let us compute the probability P_C.

Note that:
$$P_C(c) = \sum_{m,k} P_{C,M,K}(c, m, k) \quad \text{(marginal from joint law)}$$
$$= \sum_{m,k} P_{MK}(m,k) \, P_{C|MK}(c|m,k) \quad \text{(joint to conditional)}$$
$$= \sum_{m,k} P_M(m) \, P_K(k) \, P_{C|MK}(c|m,k).$$

The pairs (m,k) can take 4 possible values: $(0,0)$ $(0,1)$ $(1,0)$, and $(1,1)$.

Let $c=0$:
$$P_C(0) = \mathbb{P}(C=0) = \underbrace{P_M(0)}_{=(1-p)} \underbrace{P_K(0)}_{=1/2} \underbrace{P_{C|MK}(0|0,0)}_{=1}$$
$$+ P_M(0) P_K(1) \cancel{P_{C|MK}(0|0,1)}_{=0} \quad \text{impossible}$$
$$+ P_M(1) P_K(0) \cancel{P_{C|MK}(0|1,0)}_{=0} \quad \text{impossible}$$
$$+ \underbrace{P_M(1)}_{=p} \underbrace{P_K(1)}_{=1/2} \underbrace{P_{C|MK}(0|1,1)}_{=1}$$

Hence, $P_c(0) = \frac{1}{2}(1-p) + \frac{1}{2}p = \frac{1}{2}$.

To end the proof, note that

$$P_c(0) + P_c(1) = 1$$

then, $P_c(1) = 1 - P_c(0) = \frac{1}{2}$

which completes the proof.

(Note that this is true whatever the value of p).

Question 3:

Let $m, c \in \{0,1\} \times \{0,1\}$

$$\begin{aligned}
P_{MC}(m,c) &= \mathbb{P}(M=m, C=c) \\
&= \mathbb{P}(M=m)\ \mathbb{P}(C=c \mid M=m) \\
&= P_M(m) \cdot \mathbb{P}(K = c \oplus m \mid M=m) \quad \rightarrow \begin{pmatrix} C = k \oplus n \\ \Rightarrow k = c \oplus M \end{pmatrix} \\
&= P_M(m) \cdot \mathbb{P}(k = c \oplus m) \quad \longrightarrow k \text{ independent from } m. \\
&= P_M(m)\ P_K(c \oplus m) \quad k \text{ is uniform.} \\
&= P_M(m) \cdot \frac{1}{2}
\end{aligned}$$

Question 4:

We have that

$$\begin{aligned}
P_{MC}(m,c) &= P_M(m) \cdot \frac{1}{2} \\
&= P_M(m) \cdot P_C(c)
\end{aligned}$$

Hence, M and C are independent, which implies that $I(M;C) = 0$.

Part 2 of the exercise:

Question 1: By definition:

$$\begin{aligned}
I(M_1 M_2 ; C_1 C_2) &= H(M_1 M_2) - H(M_1 M_2 \mid C_1 C_2) \\
&= H(M_1) + H(M_2) - H(M_1 M_2 \mid C_1 C_2) \quad \begin{pmatrix} M_1 \perp\!\!\!\perp M_2 \\ \text{independent} \end{pmatrix} \\
&= 2H(M) - H(M_1 M_2 \mid C_1 C_2) \quad \begin{pmatrix} H(M_1) = H(M_2) \\ = H(M) \end{pmatrix}
\end{aligned}$$

Next, let us simplify $H(M_1 M_2 | C_1 C_2)$.
By definition of conditional entropy and the chain rule

$$H(M_1 M_2 | C_1 C_2) = H(M_1 | C_1 C_2) + H(M_2 | C_1 C_2 M_1).$$

Hence: $I(M_1 M_2 ; C_1 C_2) = 2H(M) - H(M_1 | C_1 C_2) - H(M_2 | C_1 C_2 M_1).$

Question 2

Let us assume that we have already observed C_1, C_2 and M_1.
Then, since the OTP is violated ($C_1 = M_1 + k$, $C_2 = M_2 + k$) same key

$$C_1 \oplus C_2 = M_1 \oplus M_2.$$

Knowing that M_1 is already known, then M_2 can be obtained by

$$M_2 = C_1 \oplus C_2 \oplus M_1.$$

Hence, M_2 is a function of (C_1, C_2, M_1).
Hence, there is no uncertainty on M_2 knowing we already observed C_1, C_2, and M_1.
Hence $H(M_2 | M_1 M_2 C_1) = 0.$

Question 3:

Since we can admit that

$$H(M_1 | C_1 C_2) = H(M_1 | C_1),$$

and since $I(M_1 ; C_1) = 0 \Rightarrow H(M_1) = H(M_1 | C_1)$
then: $H(M_1 | C_1 C_2) = H(M_1) = H(M).$

Question 4:

Combining all 3 results:

$$I(M_1 M_2 ; C_1 C_2) = 2H(M) - \underbrace{H(M_1 | C_1 C_2)}_{= H(M)} - \underbrace{H(M_2 | C_1 C_2 M_1)}_{= 0}$$

we obtain $\boxed{I(M_1 M_2 ; C_1 C_2) = H(M)}$.