Lloyd T Kulangara
B181133CS
CSE A

For $P_2[C=c] > 0$

Now, $P_2[M=m \mid C=c] = P_2[M=m' \mid C=c] = 1/2$
(Prob. is uniform)

Using Bayes Theorem,

$$P_2[M=m \mid C=c] = \frac{P_2[C=c \mid M=m]\, P_1[M=m]}{P_1[C=c]}$$

$$= \frac{P_1[C=c \mid M=m] \cdot 1/2}{1/2}$$

$$= 1/2$$

$\therefore P_2[C=c \mid M=m] = P_1[C=c]$ — (1)

$= P_2[Enc_k(m)=c]$

Similarly $P_2[C=c \mid M=m'] = P_1[Enc_k(m')=c]$ — (2)

From (1) & (2) $\Rightarrow P_2[C=c \mid M=m] = P_1[C=c \mid M=m']$