tomando las sentencias (1) y (2) del enunciado demostraré que (1) $\iff$ (2) se cumple:

(1) $\Longrightarrow$ (2) | sabemos que $\forall C_0 \in C, \forall m_1, m_2 \in M$

$$\Pr_{K \to \bar{K}}[Enc(K, m_1) = C_0] = \Pr_{K \to \bar{K}}[Enc(K, m_2) = C_0]$$

por teorema de Bayes puedo formar esto

$$P(A|B) = \frac{P(B|A) \cdot P(A)}{P(B)}$$

$$\Longrightarrow P(B) = \frac{P(B|A) \cdot P(A)}{P(A|B)}$$

lo que trayendo para la probabilidades dadas:

$$\Pr[Enc(K, m_1) = C_0] = \frac{\Pr[Enc(K, m_2) = C_0 | m_2 = m_0] \cdot P[m_2 = m_0]}{\Pr[m_2 = m_0 | Enc(K, m_2) = C_0]}$$

y a sabiendas de que al ser dos palabras iguales no afecta la probabilidad de que la encriptación sea C_0, podemos asumir que son eventos independientes por lo tanto:

$$\Pr[Enc(K, m_1) = C_0] = \frac{\Pr[Enc(K, m_2) = C_0] \cdot P[m_2 = m_0]}{\Pr[m_2 = m_0 | Enc(K, m_2) = C_0]}$$

y como las probabilidades son iguales por (1)

$$\therefore \quad Pr[M_2 = m_0 \mid Enc(k, m_2) = C_0] = Pr[m_2 = m_0]$$

con m_2 un $m \in M$ cualquiera //

(2) $\Rightarrow$ (1) | sabemos que

$$Pr[M = m_0 \mid Enc(k, m) = C_0] = Pr[M = m_0]$$

esto nos dice que son eventos independientes, y por lo tanto, al usar el teorema de bayes, esto se puede reescribir como:

$$\frac{Pr[Enc(k, m) = C_0 \mid M = m_0] \cdot Pr(M = m_0)}{Pr[Enc(k, m) = C_0]} = Pr[m = m_0]$$

y sabiendo que son eventos independientes, entonces:

$$Pr[Enc(k, m) = C_0] \cdot Pr[m = m_0] = Pr[Enc(k, m) = C_0] \cdot Pr[m = m_0]$$

para 2 $m \in M$, se cumple

(1) // por lo tanto se cumple (1) $\Leftrightarrow$ (2) ∎