

**Problem 1):** We know that the expression

$$\Pr[M = m | C = c] = \Pr[M = m], \quad (1.1)$$

which holds for some encryption scheme  $(\text{Gen}, \text{Enc}, \text{Dec})$ . We apply Bayes' formula to the left-hand-side of expression 1.1 to yield

$$\Pr[M = m | C = c] = \frac{\Pr[M = m, C = c]}{\Pr[C = c]} \quad (1.2)$$

Since the  $\Pr[M = m, C = c]$  term in expression 1.2 represents a Joint Probability Distribution, we also have

$$\Pr[M = m, C = c] = \Pr[M = m] \Pr[C = c | M = m]$$

This allows the result in expression 1.2 to be equivalently expressed as

$$\Pr[M = m | C = c] = \frac{\Pr[M = m] \Pr[C = c | M = m]}{\Pr[C = c]}$$

which is divided by  $\Pr[M = m]$  to give

$$\frac{\Pr[M = m | C = c]}{\Pr[M = m]} = \frac{\Pr[C = c | M = m]}{\Pr[C = c]} \quad (1.3)$$

By noting that expression 1.1 implies

$$\frac{\Pr[M = m | C = c]}{\Pr[M = m]} = 1,$$

the result in expression 1.3 becomes

$$\frac{\Pr[C = c | M = m]}{\Pr[C = c]} = 1$$

Multiplying this result by  $\Pr[C = c]$  gives

$$\Pr[C = c | M = m] = \Pr[C = c], \tag{1.4}$$

thereby proving that  $\Pr[M = m | C = c] = \Pr[M = m]$  implies  $\Pr[C = c | M = m] = \Pr[C = c]$ .

□