CSC 429 Assignment 1

Alexander Williams

January 19, 2025

Question 5

a)

Proof by contradiction.

Assume that for all message distributions M_1, M_2 on message pairs $m_1, m_2 \in \mathcal{M}$ and all $c_1, c_2 \in \mathcal{C}$ where $P[C_1 = c_1 \wedge C_2 = c_2] > 0$:

$$Pr[M_1 = m_1 \wedge M_2 = m_2 | C_1 = c_1 \wedge C_2 = c_2] = Pr[M_1 = m_1 \wedge M_2 = m_2]$$

START BAYES HERE

First, let's look at the probability $Pr[C_1 = c \wedge C_2 = c | M_1 = m_1 \wedge M_2 = m_2]$. Using Baye's rule, this can be re-written as:

$$\frac{Pr[M_1 = m_1 \wedge M_2 = m_2 | C_1 = c_1 \wedge C_2 = c_2] \cdot Pr[C_1 = c_1 \wedge C_2 = c_2]}{Pr[M_1 = m_1 \wedge M_2 = m_2]}$$

Using our assumption above, this can be simplified:

$$= \frac{Pr[M_1 = m_1 \wedge M_2 = m_2] \cdot Pr[C_1 = c_1 \wedge C_2 = c_2]}{Pr[M_1 = m_1 \wedge M_2 = m_2]}$$

$$= Pr[C_1 = c_1 \wedge C_2 = c_2]$$

Now, let's choose $c_1 = c_2 = c$, and $m_1 \neq m_2$.

$$Pr[C_1 = c \wedge C_2 = c | M_1 = m_1 \wedge M_2 = m_2]$$

$$= Pr[Enc_K(m_1) = c \wedge Enc_K(m_2) = c | M_1 = m_1 \wedge M_2 = m_2]$$

Since we are conditioning on the event that $M_1 = m_1 \wedge M_2 = m_2$, we can simplify:

$$= Pr[Enc_K(m_1) = c \wedge Enc_K(m_2) = c]$$

Since the same key k cannot encrypt two messages into the same ciphertext,

$Pr[C_1 = c \wedge C_2 = c | M_1 = m_1 \wedge M_2 = m_2] = Pr[Enc_K(m_1) = c \wedge Enc_K(m_2) = c] = 0$

This is a contradiction, as

$$Pr[C_1 = c \wedge C_2 = c | M_1 = m_1 \wedge M_2 = m_2] = Pr[C_1 = c_1 \wedge C_2 = c_2]$$

which is greater than zero, and

$Pr[C_1 = c \wedge C_2 = c | M_1 = m_1 \wedge M_2 = m_2] = Pr[Enc_K(m_1) = c \wedge Enc_K(m_2) = c]$

which is equal to zero
Thus, no encryption scheme can satisfy this definition.

b)