CS 171: Discussion 2 (Jan 29)

1. Equivalence of Definitions

You are given an encryption scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ with message space $\mathcal{M}$ that satisfies the condition

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

for every probability distribution M over $\mathcal{M}$, every message $m \in \mathcal{M}$, and every ciphertext $c \in \mathcal{C}$ such that $\Pr[C = c] > 0$. Show that for any two messages $m, m' \in \mathcal{M}$ and for any $c \in \mathcal{C}$,

$$\Pr[\mathsf{Enc}(K, m) = c] = \Pr[\mathsf{Enc}(K, m') = c]$$

2. A Different One-time Pad

Consider the following encryption scheme for the message space $\{0,1\}$.

- Gen: Choose two random bits $a, b \xleftarrow{\$} \{0,1\}$.
- $\mathsf{Enc}((a,b),m)$: Choose random $x_1 \xleftarrow{\$} \{0,1\}$ and compute x_2 such that $a \cdot x_1 + b + x_2 = m$ where $+$ and $\cdot$ are operations over $\mathsf{GF}(2)$.
- $\mathsf{Dec}((a,b),(x_1,x_2))$: Compute $m = a \cdot x_1 + b + x_2$.

Show that this scheme is perfectly secure. *Hint: Use the second (equivalent) definition of perfect secrecy from Q1.*

3. Non-Negligible Function

A function $f : \mathbb{Z}^+ \to [0,1]$ is a *negligible function* if $\forall$ polynomials $p(\cdot)$, $\exists N \in \mathbb{Z}^+$ such that $\forall n > N$ we have $f(n) < \frac{1}{p(n)}$.
Define a non-negligible function using the negation of the definition of a negligible function.
See `https://en.wikipedia.org/wiki/Universal_quantification`.