Perfect Secrecy (A Minor Correction)

This was the definition that I originally forgot to give, then filled in later (correctly, as it turns out).

Definition 0.1. Define the *set of possible ciphertexts for a given key K* as the set given by $C(K) = \{E_K(M) : M \in \mathcal{M}\}$

Unfortunately, after giving this definition, I changed the definition for $p(C)$ (the probability of seeing the ciphertext C) to something slightly wrong. The corrected definition is this:

$$p(C) = \sum_{\substack{K \\ C \in C(K)}} p(K) p(D_k(C)) \ .$$

Here, $p(K)$ is the probability that the key K is chosen, and $p(D_k(C))$ is the probability that a message M (that encrypts to C under key K) is sent. In class, I erroneously introduced a variable y in place of C.

Since I have your attention, I may as well give the proof that I skipped.

Theorem 0.1 (Our two definitions for perfect security are equivalent)**.**

$$p(M \mid C) = p(M) \Longleftrightarrow p(C \mid M) = p(C) \quad \textit{for all } M, C$$

Proof. To see this, note the following:

$$\begin{aligned} p(M, C) &= p(C, M) && \text{joint probabilities} \\ p(M, C) &= p(M \mid C) p(C) && \text{identity} \\ p(C, M) &= p(M) p(C \mid M) && \text{identity} \\ p(M) p(C \mid M) &= p(M \mid C) p(C) && \text{Bayes' Theorem.} \end{aligned}$$

($\Longrightarrow$) If we have perfect secrecy, by definition $p(M) = p(M \mid C)$, so those two terms cancel and we have

$$p(C \mid M) = p(C)$$

as claimed. The other direction is identical. □