Introduction to mathematical cryptography
Homework problems
Week 12

23. Assume Alice and Bob apply the XOR cipher on t bits (and they use a key only once to keep security). Prove that if both M and K are independent uniform distributions (i.e. for any $m \in M$, $k \in K$, $\mathrm{P}(M = m) = \mathrm{P}(K = k) = 2^{-t}$, $\mathrm{P}(M = m, K = k) = 2^{-2t}$), then they achieve perfect secrecy.

24. Consider the 1-bit XOR cipher, i.e. $\mathcal{M} = \mathcal{K} = \mathcal{C} = \{0, 1\}$, and $e_k(m) = m \oplus k$, $d_k(c) = c \oplus k$. Assume M and K are independent random variables (i.e. for any $m \in \mathcal{M}, k \in \mathcal{K}$, $\mathrm{P}(M = m, K = k) = \mathrm{P}(M = m)\mathrm{P}(K = k)$) such that $\mathrm{P}(M = 0) = p$, $\mathrm{P}(K = 0) = q$ for some parameters $0 \leq p, q \leq 1$ (of course, this implies $\mathrm{P}(M = 1) = 1 - p$, $\mathrm{P}(K = 1) = 1 - q$). Compute the values of the density functions f_M, $f_{M|C}$, and determine the pairs (p, q) which give rise to perfect secrecy.

Note: Please, provide complete arguments everywhere, and explain how you arrived at your answer/solution. Giving the result without explanation leads to score deduction.