Introduction to mathematical cryptography
Homework problems
Week 10

19. 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 $m \in M$, $k \in K$, $\Pr(M = m) = \Pr(K = k) = 2^{-t}$, $\Pr(M = m, K = k) = 2^{-2t}$), then they achieve perfect secrecy.

20. Consider the 1-bit XOR cipher, i.e. $\mathscr{M} = \mathscr{K} = \mathscr{C} = \{0,1\}$, 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 $m \in \mathscr{M}, k \in \mathscr{K}$, $\Pr(M = m, K = k) = \Pr(M = m)\Pr(K = k)$) such that $\Pr(M = 0) = p$, $\Pr(K = 0) = q$ for some parameters $0 \leqslant p, q \leqslant 1$ (of course, this implies $\Pr(M = 1) = 1 - p$, $\Pr(K = 1) = 1 - q$). 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.