# Minimum Key Length for Perfectly Secure Encryption

It turns out to be impossible to design an encryption scheme that provides both perfect security and short keys. So even though the one-time pad may seem inefficient, its key length is optimal for a perfectly secure scheme.

Theorem (Shannon, 1949)

For any perfectly secure encryption scheme, it holds that $H(K) \geq H(M)$.

Proof

Again, we turn to entropy diagrams. Write $a = I(M; C|K) \geq 0$. using the fact that $I(M; K) = 0$ (setup assumption) and $I(M; C) = 0$ (security), we can fill in the entropy diagram as follows:
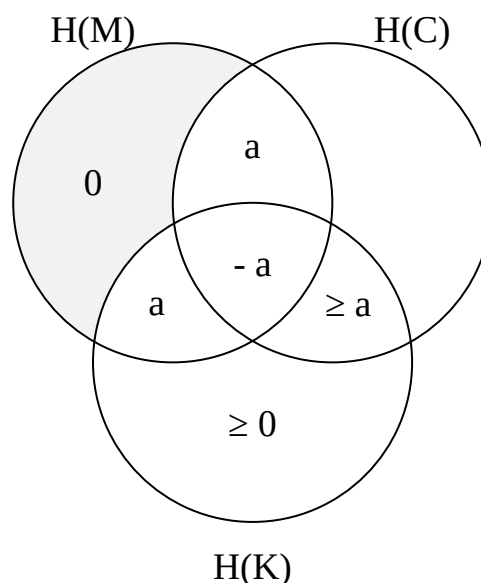
Note that $I(K; C|M) \geq a$ follows from the fact that $I(C; K) \geq 0$ and $R(C; K; M) = -a$. From the diagram, we observe that $H(M) = a$, and that $H(K) \geq a$. Hence, $H(K) \geq H(M)$.