XOR cipher

Come One-Time Pad, ma non cambiamo la chiave ad ogni messaggio.

Problema:

$$
\begin{array}{ll}
c_1 = m_1 \oplus k & \oplus \\
c_2 = m_2 \oplus k & = \\
\hline
c_1 \oplus c_2 = m_1 \oplus k \oplus m_2 \oplus k & \\
\quad = m_1 \oplus m_2 \oplus 0 & \\
\quad = m_1 \oplus m_2 &
\end{array}
$$

Permette ad esempio di determinare se è stato mandato lo stesso messaggio (lunghe sequenze di 0 in $m_1 \oplus m_2$).