Masque jetable

Obtention de la clé

- Une fois qu'on connait m_1 ou m_2 on peut facilement retrouver la clé k

$$
\begin{aligned}
c_1 \oplus m_1 &= (m_1 \oplus k) \oplus m_1 \\
&= k \oplus \cancel{m_1 \oplus m_1} \\
&= k
\end{aligned}
\qquad
\begin{aligned}
c_2 \oplus m_2 &= (m_2 \oplus k) \oplus m_2 \\
&= k \oplus \cancel{m_2 \oplus m_2} \\
&= k
\end{aligned}
$$

Rencontre par le milieu