Masque jetable

Déchiffrement des messages 1 et 2

- Astuce: En XORant les cryptogrammes 1 et 2 ensemble on obtient le XOR des messages

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

- On peut donc isoler m_1 en essayant différents $m \in \{m_a, m_b, m_c, m_d\}$

$$\begin{aligned} m_1 \oplus m_2 \oplus m &= m_1 \oplus \cancel{m_2 \oplus m} \\ &= \begin{cases} m_1 & \textbf{si } m = m_2 \\ ? & \textbf{sinon} \end{cases} \end{aligned}$$

Masque jetable

Obtention de la clé

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

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