Masque jetable

Mise en situation

- On sait que c_i sont des chiffrés sous une (même !!!) clé inconnue k de messages m_i inconnus

$$c_1 = m_1 \oplus k$$
$$c_2 = m_2 \oplus k$$
$$c_3 = m_3 \oplus k$$

- Mais c_2 fait parti d'un ensemble de messages connus (poèmes québécois)

$$m_2 \in \{m_a, m_b, m_c, m_d\}$$

Masque jetable

Déchiffrement des messages 1 et 2

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

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