Masque jetable

Exemple XOR

- Pour chiffrer le message “hello” avec la clé “world” on calcule

```
  hello
⊕
  world
```

```
  104 101 108 108 111
⊕
  119 111 114 108 100
```

```
  01101000 01100101 01101100 01101100 01101111
⊕
  01110111 01101111 01110010 01101100 01100100
-----------------------------------------------
  00011111 00001010 00011110 00000000 00001011
```

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)

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