Masque jetable

Aussi appelé le chiffre parfait, ou chiffre de Vernam

- Le **masque jetable** (de l'anglais **One Time Pad**) est un schéma de chiffrement tel que

$$Enc_k(m) = m \oplus k$$

- On dit que le masque jetable est **inconditionnellement sur** si la clé utilisée est
  - Aussi longue que le message
  - Jamais réutilisée pour aucun autre message

Masque jetable

Table de XOR et propriétés

$\oplus$	**0**	**1**
0	0	1
1	1	0