

OTP - One Time Pad

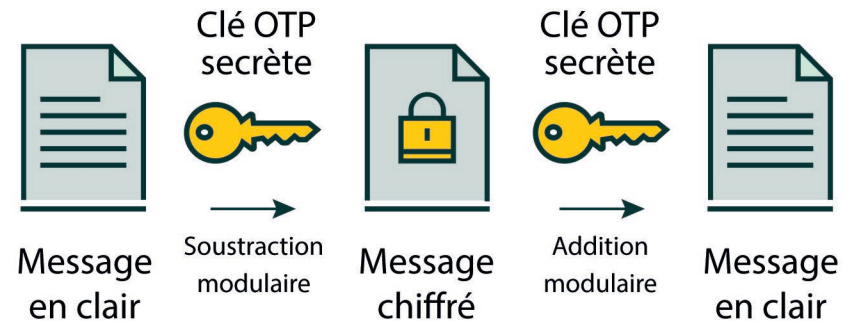
Clé OTP

27793 33873 22989 05220 80984
29034 63759 54704 97520 83781
89034 48542 47954 96699 68704
82608 71429 65813 72721 01247

Une même clé pour chiffrer et déchiffrer.

Une clé OTP est constituée de chiffres aléatoires regroupés par blocs de 5 par simple souci de lisibilité. La longueur de la clé doit être au moins égale à celle du message à chiffrer.

Chiffrer - Déchiffrer



L'OTP ou Chiffre de Vernam

Un chiffrement par OTP numérique fonctionne avec une clé secrète unique constituée de chiffres de 0 à 9. Le chiffrement se fait par soustraction modulaire et le déchiffrement par addition modulaire (modulo 10).



Le chiffrement par OTP est dit « parfait » car, si toutes les règles sont respectées, le message chiffré est indéchiffrable quelle que soit la puissance informatique utilisée et le temps passé à tenter de décrypter.