Le chiffrement par masque jetable (one-time-pad)

F. Kany. ISEN-Brest. La Croix-Rouge.

Présentation

Consulter l'article de wikipedia : `https://fr.wikipedia.org/wiki/Masque_jetable`.

1. Créer une fonction `generation_clef(message)` qui prend en argument un message sous forme d'une chaîne alpha-numérique et qui renvoie une chaine de caractères aléatoires de même longueur constituée de lettres entre A et Z. Rappel sur les codes ASCII : `ord(''A'')=65` et `ord(''Z'')=90` ; l'opération inverse est `chr`.
2. Créer une fonction `one_time_pad(message,clef)` qui prend en argument un message sous forme d'une chaîne alpha-numérique et une clef générée par la fonction `generation_clef(message)` et qui renvoie une chaine de caractères correspondant au message crypté. Rappel : pour effectuer l'opération $\oplus$ (XOR), il faut utiliser l'opérateur `^` (qui n'a rien à voir avec la puissance qui s'écrit `**`), on a : `0^0=0; 0^1=1; 1^0=1; 1^1=0`.
3. Vérifier qu'en appliquant le même clef et la même fonction de codage au message chiffré, on obtient bien le message déchiffré.