

WRITE UP CHALLENGE 'Orcs' - Rédigé par Hugo

1ère étape : Ouvrir les deux fichiers, constater qu'ils sont identiques à l'oeil nu...

2ème étape : Rechercher un script qui le fait, ou simplement en faire un soit même

3ème étape : Commande : `cmp -l -b ORIGINAL.txt PÂLECOPIE.txt`

```
hugo@pop-os:~/Desktop/COURS/CTF/CRYPTO$ cmp -l -b ORIGINAL.txt PÂLECOPIE.txt
132 154 l      61 1
269 157 o      60 0
329 154 l      61 1
685 154 l      61 1
884 130 X      170 x
1157 113 K      153 k
1865 73 ;      154 l
2074 157 o      71 9
2486 54 ,      55 -
2849 143 c      71 9
3309 157 o      60 0
3510 154 l      61 1
3514 60 0      71 9
3555 73 ;      55 -
3614 117 0      60 0
3709 157 o      143 c
3750 73 ;      61 1
3855 157 o      144 d
3870 54 ,      55 -
3950 144 d      71 9
3951 117 0      60 0
3966 60 0      157 o
4034 154 l      146 f
4045 56 .      55 -
4048 154 l      144 d
4080 143 c      145 e
4100 117 0      60 0
4189 157 o      144 d
4301 157 o      145 e
4377 157 o      60 0
4383 154 l      61 1
4405 153 k      143 c
4477 170 x      141 a
4686 117 0      60 0
4914 143 c      145 e
4987 143 c      66 6
```

4ème étape : Rassembler le flag, représenté par les différences de la deuxième colonne.

5ème étape : On s'attend à avoir un chiffrement avec une clé car dans l'énoncé il y a 'FORCE ET HONNEUR'.

C'est donc un chiffrement par transposition.

CHIFFRE PAR TRANSPOSITION

Cryptographie > Chiffrement par Transposition
Chiffre par Transposition

DÉCHIFFREMENT PAR TRANSPOSITION

★ MESSAGE CHIFFRÉ PAR TRANSPOSITION ⑦
1011xkl9-9019-0c1d-90of-de0de01ca0e6

★ CONSERVER LES ESPACES, LA PONCTUATION ET AUTRES CARACTÈRES

★ LANGUE (PRÉSUMÉE) DU TEXTE CLAIR Français

MÉTHODE DE DÉCHIFFRER

CONNAISSANT LA CLÉ OU LA PERMUTATION DE CHIFFREMENT
FORCE ET HONNEUR
→ (4,5,6,12,1,8,10,11,2,9,3,14,7,13) → (5,9,11,1,2,3,13,6,10,7,8,4,14,12)⁻¹

TENTER TOUTES LES PERMUTATIONS (BRUTEFORCE JUSQU'A TAILLE 6) ⑦

SENS D'ÉCRITURE/LECTURE LORS DU CHIFFREMENT

SENS Ecriture en lignes, Lecture par colonnes (par défaut)

► DÉCHIFFRER

Voir aussi : Substitution Mono-alphabétique

Une fois déchiffré avec 'FORCE ET HONNEUR', il faut entourer le flag par NHM2I{}.

Flag : NHM2I{106XOKF9011A9E0D1E0D09019ECCLD01}