

USB MOYEN

On ne peut pas exécuter la commande **sudo mount -o loop dest**. Ainsi, les étapes nécessaires sont les suivantes :

1/Utiliser la commande **sudo cryptsetup luksOpen usb.img usb_crypt**. Un mot de passe est requis, et il est possible de créer une liste de mots de passe avec un script pour effectuer une attaque par force brute, ou simplement deviner le mot de passe, qui est "super-secret".

2/Exécuter **sudo mount /dev/mapper/usb_crypt dest**.

3/À l'intérieur, découvrir un fichier flag.txt. La première ligne est une ligne normale du type : bonjour. bye. La deuxième ligne est chiffrée en **ROT47** et doit être déchiffrée. En déchiffrant cette ligne, on obtient un autre message chiffré.

4/ Ainsi, pour le déchiffrer, il est nécessaire de comparer la première ligne avec la seconde. Il est évident qu'un algorithme de substitution a été utilisé, et il faut écrire l'algorithme inverse de substitution en remplaçant chaque lettre par sa lettre correspondante (par exemple, remplacer "k" par "b" et ainsi de suite).

5/Le flag est trouvé.