Le piège Huffman-XOR

Cette énigme a été créée par **Cogite**

Lucka Blindi, utilisateur assidu du site, affirme avoir résolu l'un des plus anciens problèmes de la cryptographie : s'affranchir de la contrainte de longueur de clef du masque jetable. Il vient de poster ce message provocateur sur le forum général, provoquant une vive réaction de la communauté :
« Le masque jetable est obsolète : j'ai trouvé mieux. En comprimant d'abord le message avec un code de Huffman statique, j'en réduis la redondance. J'applique ensuite un XOR périodique sur le flux binaire obtenu. Le résultat ? Un chiffrement aussi robuste qu'un masque jetable, avec une clef qui tient dans la poche. »
Lucka Blindi vous met au défi de décrypter son chef-d'œuvre.

Codebook Huffman :
E=000, _=001, A=0100, I=0101, L=0110, N=0111, O=1000, R=1001, S=1010, T=1011, U=1100, C=11010, D=11011, M=11100, P=11101, B=1111000, F=1111001, G=1111010, H=1111011, Q=1111100, V=1111101, X=1111110, Y=11111110, Z=111111110, J=1111111110, K=11111111110, W=11111111111

Cryptogramme (hexadécimal) :
BE0AF6C395756BD0B432F9BC95FEBEC43D237B7F9305FB7BA6A2F544BC
9794C871FDBA8757E80CDD300A46605FAD5C3AD797A7E80D72950958D
E9E8FDED9C846A12FCFA37246A1A4D38E77FC52CD955EF288914BB6AE2
ED400A525736C61CB584BF55B0EF9DCC0099F72F2E23510B49A7AFDDC8
2BC88734388AD0B2F714FCA5CD3E9B948A2A0EB891AD1BE341FA41C71

6C432D0E2A876FC6CFE0C98807C26EC364982899CF2620A9047A5AE8BC
9F11A0EB378ABFA6AAD02F618E3450D82D1227258C6B55D020C668EB17
C86F646254D7862BDB3C8A4B6FE652879644E829B7EAADCE32044F3E02
C53C042CF74D26B6DDF9E3BD22958DCB17305FD8E9CB063771C118F9B8
0D204749E7E596E60150A666BE04C6FACFBD44F27F1975E32CB0E9B9A8
53C9A36EBC6F921BDA3A7900

Notes techniques :
- Le flux binaire est obtenu par concaténation des codes de Huffman.
- La clef XOR est appliquée de manière périodique ; sa longueur ne dépasse pas 80 bits.
- Le cryptogramme est fourni en hexadécimal.
- Les derniers bits peuvent ne pas être alignés sur des codes Huffman complets (padding).
- La réponse utilise la même convention que le codebook.

Lucka Blindi affirme avoir conçu un chiffrement incassable. Saurez-vous percer son secret ?