Bien secret ?

Cette énigme a été créée par **mvc**

Alice, passionnée par la cryptographie, a mis au point une nouvelle méthode pour protéger ses messages. Elle ne souhaite plus utiliser les méthodes classiques qu'elle juge trop prévisibles.

Alice prend son message (code en UTF-8) et le découpe en segments de 8 octets. Pour chaque segment, elle génère une clé pseudo-aléatoire à l'aide d'un générateur congruentiel linéaire (LCG, de formule $x_n = a*x_{n-1} + b$) dont les paramètres sont fixés ($a = 2^{61} – 1$, $b = 2^{31} - 1$ et $m = 2^{64}$) Elle applique ensuite un OU exclusif (XOR) entre le segment de son message et la valeur générée. Enfin, elle exporte le tout dans un fichier hexadécimal.

La clé correspond à la graine initiale du générateur. Mais Bob lui fait remarquer que dans ce cas ce n'est pas une bonne idée de signer ses messages "Ton Alice".

Pouvez-vous décoder le message suivant ?

3effadfe22a3b8bdc40e1c53574346167effadff2caca4a7684116061257f19f
dc5d24ff2cbba8bc1f41131ff19953423df7ffe86daebbacae41161641105f5
798ebfeee38a3a8ba0d0406535f595c43e1fdf8e128bce3e9c40d52155359
461646ece2fd6daca5a8980552035d4540161137eeff24bda8e93d0d07001
c1066591cbecce124aca8