

Insecure Keith - Alan Yan

The only difficulty in this problem is figuring out the encryption scheme. Translating $K \rightarrow 1, T \rightarrow 0$ we are given a vector of bytes and the number 283 in binary is 100011011. This is a well-known for being associated with the irreducible polynomial $x^8 + x^4 + x^3 + x + 1$ in $GF(2^8)$. Hence, the encryption scheme is [AES](#) where the key is "*You are the key!*". We can decrypt it now to get the flag "HOMEOMORPHISMS!1"

¹



¹ Taken from [wikipedia](https://en.wikipedia.org/wiki/Alan_Yan)