MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

Kaskade-S/T - Part 2

Author: Bernhard Esslinger

February 2011

Kaskade

Your friend calls you again and wants you to "test" his cipher (see Kaskade-S/T - Part 1) with a longer key. He again sends you a plaintext and the corresponding ciphertext, and asks, if you could find out the key used for encryption.

Instead of a key length of 2*26 byte, this time your friend uses a key length of 2*256 byte. Additionally this time he uses different keys for the substitution and the transposition.

Challenge

Now, the cipher processes the plaintext and the ciphertext in blocks of a length of 256 byte and pads the last block, if necessary, with X.

The solution of this challenge is the key, which has been used to encrypt the given plaintext (you have to give it in hex format without delimiter, also without the commonly used “0x” prefix in front of hex values, for example 120a...).

Challenge

If you write the key you found into the file "256key", you are able to test with the given Python v3.1 program (Kaskade.py), whether the given plaintext can be encrypted correctly into the given ciphertext.

The call for encryption is:

```
python3.1 Kaskade.py -e plaintext ciphertext 256key
```

The call for decryption is:

```
python3.1 Kaskade.py -d ciphertext plaintext 256key
```