MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

Kaskade-S/T - Part 4

Author: Bernhard Esslinger

May 2011

Kaskade

Your friend has seen that *Kaskade - Part 3*, which uses two permutations of length 256, was solved already, so he tries to further advance his cipher.

To achive this, his first idea is to encrypt a ZIP archive, instead of a plaintext, to hide possible patterns of the plaintext.
In the additional file of this challenge (*mtc3-esslinger-12-kaskade4-add.zip*) you can find a ZIP archive, which was encrypted by your friend (*ciphertext-KST4*).

Furthermore, there is the Python v3.1 program *Kaskade.py*, with which you can test the decryption and encryption.

Challenge

Decrypt the given ciphertext file and unpack the contents of the ZIP archive. The key used here consists of two 256-permutations of the type "Random-Different".

The solution to this challenge is the last word of the first English paragraph of the text and the last word of the first German paragraph. Please provide the solution case-sensitive and separate the two words with a single space.

Hint: You know that your friend is momentarily working on power grids.

Kaskade.py

With the given Python program you are able to test whether the given ciphertext can be decrypted correctly into the sought-after plaintext. Here, "Key" is a file which contains the key.

The call for encryption is:

```
python3.1 Kaskade.py -e plaintext-KST4.zip ciphertext-KST4 Key
```

The call for decryption is:

```
python3.1 Kaskade.py -d ciphertext-KST4 decrypted-text-KST4.zip Key
```