MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

KASKADE-S/T - PART 5

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 second idea does not need the user to create a ZIP archive of the plaintext first, as in *Kaskade - Part 4*, but he improved the cipher to use several iterations (rounds) instead.
In the additional file of this challenge (*mtc3-esslinger-13-kaskade5-add.zip*) you can find a text, which was encrypted by your friend (*ciphertext-KST5*).

Furthermore, there is a Python v3.1 program *Kaskade.py*, with which you can test the decryption and encryption (see last page).

Challenge

Decrypt the given ciphertext. To do this you need the key that was used. The key used here consists of two 256-permutations of the type "Random-Different", and the number of iterations (rounds) is 10.

The solution to this challenge is the name of the civilizing achievement mentioned in the text (written in quotation marks). Please provide the English name as well as the German name, separated by a single space. Please provide the names as written in the plaintext.

Hint: You know that your friend is momentarily interested in Fukushima und Chernobyl.

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-KST5.txt ciphertext-KST5 Key -r 10

The call for decryption is:

python3.1 Kaskade.py -d ciphertext-KST5 decrypted-text-KST5 Key -r 10