MysteryTwister C3
THE CRYPTO CHALLENGE CONTEST

Brute-Force-Attack on Triple-DES with reduced key space

Author: Nina Schöllhammer

October 2010

Triple-DES

In 2006, a machine based on re-configurable integrated circuits (FPGAs) was designed to accelerate cryptographic brute-force-attacks significantly. This machine was able to complete a brute-force-attack on a DES key (56 Bit) in less than a week. The costs of USD 10,000 for this machine were considerably low, compared to similar machines like "Deep Crack" from 1998 for USD 250,000.

However, for Triple-DES none of these machines could succeed in a brute-force-attack. But if the key was not generated randomly or parts of the key can be guessed, the key space will be significantly reduced so that a brute-force attack may succeed even for Triple-DES.

Challenge

For this challenge the key was not generated randomly but chosen in a way that it can be reconstructed easily:
The author just used the name of the described machine built in 2006 and added six meaningful digits.
Then he converted this string, containing characters and digits, into hex representation and used the result as key. In the text file for this challenge you can find a ciphertext (*mtc3-shoellhammer-01-3des.txt*), encrypted with this key using 2-Key Triple-DES (CBC). The first line of the plaintext is the solution to this challenge.