

# MysteryTwister C3

A CRYPTO CHALLENGE BY CRYPTOOL

## WORLD RECORD CHALLENGE

Who will set the new world record in an exhaustive key search?

*Klaus Schmeh*

**The longest key that has ever been publicly cracked by exhaustive key search was 64 bits long. This world record was set by a team of experts in 2002 after five years of computation. More information is available at Wikipedia (see „RSA Secret-Key-Challenge“).**

**The purpose of this challenge is to improve the current world record by one bit. This means that a 65-bit key is to be cracked. As computer technology has considerably improved since 2002, it should be possible to solve this challenge in less than five years.**

The ciphertext given below was encrypted with CrypTool. The encryption algorithm used is AES in ECB mode with a key length of 128 bits. The first 65 bits must be guessed. The remaining 63 are all set to 1.

Your task is to guess the first eight bytes of cleartext. They form an English word written in capital ASCII letters, and this is the codeword for the challenge. The remaining eight bytes have the value „CrypTool“ (in ASCII code) or 43 72 79 70 54 6F 6F 6C (in hex code).

Here is the ciphertext (in hex code):

**4B 14 55 BC 8D DF 33 AF 57 91 53 90 BB 2C E1 2A**