MysteryTwister C3
THE CRYPTO CHALLENGE CONTEST

CMEA Part II

Author: Mark Stamp

December 2010

CMEA - Cellular Message Encryption Algorithm

CMEA is a block cipher which operates on blocks of the size of 2 to 6 bytes. CMEA was one of the four cryptographic primitives used in the mobile communications network in the US. The key length of CMEA is 64 bit.
1997 some attacks on CMEA were published and showed that CMEA has several weaknesses. There were accusations that those weaknesses were built in by the NSA, but they denied any role in the design of the algorithm.

There is a *known-plaintext attack* which recovers the key (and thus the whole plaintext) given only 40 to 100 known plaintext blocks.

Challenge

Your challenge is to perform a *known-plaintext attack* on CMEA. You find the ciphertext (cmea2Cipher.txt.zip) and the initial 40 plaintext blocks (cmea2InitPlain.txt) within the zip archive of this challenge. Furthermore, the zip archive contains an implementation (CMEA_code.zip) written in C.

For this challenge a block size of 3 byte was used, as it was common in the US to encrypt each dialed digit this way.

The solution to this challenge is the complete plaintext.