MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

ORYX STREAM CIPHER – PART 1

Author: Mark Stamp

July 2010

Challenge

The ORYX Stream Cipher is used in the US for encrypting mobile communication. The given keystream was generated with the standard L permutation.
Recover the 96-Bit key, which conists of the initial fillings of the 3 LFSRs X, A, B used within the ORYX cipher.
The wanted password are the 3 fillings in hexadecimal written as one word, e.g.: X||A||B.

You find the keystream and the L permutation in the zip-archive for this challenge, the filename is out_ORYX1.txt.

Hint: Pay special attention on the implementation of the ORYX cipher used here. Look for the direction the shifts are performed and the function that extracts the highest 8 Bit! The sourcecode is contained in the zip-archive as well, the filename is ORYX_code.zip