AKELARRE – PART 1

Author: Mark Stamp

November 2010
Akelarre

Akelarre is a block cipher, which operates on blocks of the size 128 bit. Akelarre was published in 1996 and combines the basic design of IDEA (International Data Encryption Algorithm) with ideas of RC5. With this construction the authors wanted to combine two (presumably) strong block ciphers to create a third even stronger cipher.

Akelarre works with a variable key length and with a variable number of rounds. The authors proposed that Akelarre is secure with a key length of 128 bit and 4 rounds.

Akelarre is a good example that the combination of two strong ciphers does not necessarily create a third strong cipher: Akelarre was broken within a year after its publication. The presented attack is totally independent of the used key length or the number of rounds.
Challenge

It is your challenge to perform a \textit{known plaintext attack} on Akelarre. You find the ciphertext (akelarre1Cipher.txt.zip) and the initial plaintext (akelarre1InitPlain.txt) within the zip archive of this challenge. Furthermore, there is an implementation (Akelarre_code.zip) written in C in the zip archive.

As proposed by the authors of the cipher the given ciphertext was encrypted using Akelarre with a key length of 128 bit and 4 rounds. It is also known that the plaintext is English and consists only of ASCII characters.

The solution to this challenge is the complete plaintext.