Linear Cryptanalysis of the FEAL-4 Cipher

This assignment will involve implementing a major cryptanalytic attack on a weak block cipher (FEAL-4) to find the six secret sub-keys that have been used. This is a VERY hard assignment and will take a considerable amount of time, so please start working on it as soon as it is released.

The cryptanalytic attack can be implemented in the programming language of your choice. Your program will have to loop through a lot of different possible values, so it should be reasonably efficient. The source code for the FEAL-4 cipher (from which the six secret sub-keys have been removed) will be provided on Loop in C and Java, so you may wish to make use of this code and implement your attack in one of these languages.

Your task is to discover as many of the bits as possible of the six 32-bit sub-keys K0-K5 used in this cipher. The more bits, the more marks you will get. However, you will get some marks for even finding a few bits of the sub-keys, as this is a very difficult task. You should submit your code along with a written report describing how you went about the cryptanalysis and the results obtained through the Loop page for this module.

Percentage: 25%

Submission status

This assignment will accept submissions from **Monday, 18 October 2021, 12:00 AM**