Report
---
This challenge is to break the FEAL-4 cipher (retrieve the key used) having knowledge only of 200 known plaintext ciphertext pairs.

#### Implementation
The FealAttack class contains the components required to launch an attack on the cipher

```$xslt
// Given (plaintext,ciphertext) pairs (Pi,Ci), i = 0...n-1
for K0 = 0 to 232 - 1 // putative K0
	count[0] = count[1] = 0
	for i = 0 to n - 1
		j = bit computed in first equation for a
		count[j] = count[j] + 1
	next i
	if count[0] == n or count[1] == n then
		Save K0 // candidate for K0
	end if
next K0
```

There are 2 attempts made

1. Exhaustive search, this exhausts the full 32-bit key space searching for a list of suitable keys. The constant 'a' function is as follows:

```$xslt

a=S23,29(L0 ⊕R0 ⊕L4) ⊕ S31(L0 ⊕L4 ⊕R4) ⊕ S31F(L0 ⊕ R0 ⊕ K0)

```
Given the time required to complete an exhaustive search it did not complete within 24hrs

2. Compress the keyspace to 16bits by use of an M function

The constant 'a' function is as follows:
```$xslt
a = S5,13,21(L0⊕R0⊕L4)⊕S15(L0⊕L4⊕R4)⊕S15(F(L0⊕R0⊕K'0))
```
This function completes within a few seconds but the search is not successful.

#### Execute

Build and run FealAttack.java

#### Conclusion
The first attempt ran for 24hrs and did not complete. It is more than likely the implementation is missing a vital piece of information..

Kieran Mc Gowan