INF143A 22V – Applied Cryptography

First Mandatory Assignment

Problem 1

In this problem I used magma to find the maximum possible cycle length.

http://magma.maths.usyd.edu.au/calc/

Requested for the cycle length by typing:

```
PrimitivePolynomial(GF(2), 100);
```

And got the output:

$.1^100 + $.1^57 + $.1^56 + $.1^55 + $.1^52 + $.1^48 + $.1^47 + $.1^46 + $.1^45
+ $.1^44 + $.1^43 + $.1^41 + $.1^37 + $.1^36 + $.1^35 + $.1^34 + $.1^31 +
$.1^30 + $.1^27 + $.1^25 + $.1^24 + $.1^22 + $.1^20 + $.1^19 + $.1^16 +
$.1^15 + $.1^11 + $.1^9 + $.1^8 + $.1^6 + $.1^5 + $.1^3 + 1

Problem 2, 3, 4

These problems have been solved and written in python. To run the code, simply just open it into an editor and run from there.