Adam Hayse

CS 492 – Computer Security

Project Summary

27 March 2017

I did my project on how the AES S-box is generated, and I also performed a linear analysis on both the AES S-box and a randomly generated S-box. Here is a breakdown of what each of the programs does:

AESsbox.exe

The main function of this program is to calculate the modular inverses of the polynomials in the Galois Field 256 using an irreducible polynomial provided by the user at the start of the program, and then applying an affine transformation to get the final result. This program does many things based on the switches that you send to the program. It does not take any parameters other than the switches that you provide. -p and -w will print the S-box and write the S-box to a text file respectively. The -w switch will write the S-box to a file called AESsbox.txt. If you also call it with -i, then it will not perform the affine transformation and you will only see the inverses of each polynomials given the irreducible polynomial that you provide when you first run the program. One exclusive switch is -l (lower-case *el*), which will calculate for you all of the irreducible polynomials of degree 8. If you provide a polynomial that is not irreducible, then you will see a lot of 0x63’s because this is the result of performing an affine transformation on 0, which is the default value for inverse when a particular polynomial does not have an inverse.

Example program call: AESsbox.exe –p // Prints S-box to terminal

linearcrypt.exe

This program performs a linear cryptanalysis of the S-box that is sent to it as its first parameter. The 2nd parameter is the name of the file that you want to write to. It creates both a text file and a portable greymap file (.pgm). The .pgm file can be opened with GIMP.

Example program call: linearcrypt.exe AESsbox.txt example1

randomsbox.exe

This program simply generates a random S-box where all output elements form a one-to-one correspondence with its input elements. The results are written to a file called randomsbox.txt, which has the same format as AESsbox.txt.