Integral Encryption

Walter B. Gress V

Drexel University

Friday, June 7 2013

The concept is to encode dsat as coeffcients for use with the derivative/integral functions as trapdoors for a more difficult encryption to break.

# introduction

The purpose of this paper is to introduce a new type of encryption, denoted as Integral Encryption. In this method, the derivative and integral as a pair and inverses are used as trapdoor functions .

# method

This section consists of a description of the algorithm. Given a series of digits, a polynomial is generated, with each digit being a coefficient of a term in the trapdoor equation. The trapdoor equation is a regular polynomial. The encryption process is simple. The encryption is equivalent to taking the derivative of the equation resulting in the dropping out of the constant term(s). To recover the original equation the integral is taken and the trapdoor appended, in this case the trapdoor is the C value in the integrated equation. By knowing the C value, the full original trapdoor equation is restored in its entirety and by removing he coeffcients and

reassembling them, the original series of digits is restored.

# EXPANSION

Obviously this simple operation may be possible to solve. Instead of taking a data block of say, ten thousand bytes, and encoding that all within one polynomial, we divide the block of data into short segments, each with its own coeffcients (obviously) and each with its own unique trapdoor. The smaller the polynomial the better the encryption.

# EXAMPLE

Given the string of values 1 1 3 5 6

Given the polynomial:

x4 + x3 + 3x2 + 5x + 6

And its inverse:

4x3 + 3x2 + 6x +5

Taking the integral and reversing the process:

x4 + x3 + 3x2 + 5x + C

where C is the trapdoor.

# CONCLUSION

Instead of sending bits through multiple obfuscating boxes and operations, I have presented an efficient, effective, means of encryption using basic mathematical functions.