MATH 314 Fall 2023 - Class Notes

3/27/2024

Devyn Mason

SAES Encryption Demo

In this example, we have a plaintext of 1010 1110 0111 0001 and a k of 1110 1101 0010 0110

Additionally, w_0 = 11101101 and w_1 = 00100110

- First we calculate g(w_1) by splitting up w_1 into bits of 4:
- This gives us blocks of 0010 and 0110. We then swap their positions so 0110 is on the left, and 0010 is on the right.

- Then, feed both sides through the SBOX and change to your output. By feeding the left side through the SBOX, we get 1000 and 1010 on the right.
- In g(w_1),the right side stays the same while the left side is added to its corresponding polynomial for the round. Since this is the first round, we add polynomial $\mathrm{x}^3$to 1000.
- 1000 is to convert to the polynomial $\mathrm{x}^3 + 0x^2 + 0x + 0$.Each power has the coefficient of its corresponding bit. So if we then add $\mathrm{X}^3$to this, we get 0000. So finally, g(w_1) = 00001010.
- We can now find w_2. This is done by xoring between w_0 and g(w_1). This gives us 1110 1101 + 0000 1010 = w_2 = 11100111.
- To find w_3, we have to xor w_2 with w_1. This gives us 1100 0001 for w_3.
- We are then required to calculate g(w_3). This is done by doing the same process to find g(w_1). After doing this process, we get a value of 0111 1100.To find w_4 we xor g(w_3) with w_2 and get 1001 1011.To find w_5 we xor that value with w_3 and get 0101 1010.
- All these calculations are necessary because they give us our keys. There are as follows: $\mathrm{k}_1 = \begin{pmatrix} 1110 & 0111 \\ 1100 & 0001 \end{pmatrix}$ $\mathrm{k}_2 = \begin{pmatrix} 1001 & 1011 \\ 0101 & 1010 \end{pmatrix}$
- We then want to xor roundkey 0 with the plaintext and run that value through the SBOX. This gives us 1010 1110 0111 0001 + 1110 1101 0010 0110 = 0100 0011 0101 0111. After running this through the SBOX, we get 1101 1011 0001 0101.
- We must then conver this to polynomials and insert those ploynomials into a hill cipher as follows: $\begin{pmatrix} x^3+x^2+1 & 1 \\ x^3+x+1 & x^2+1 \end{pmatrix}$ We then perform the shift rows step: $\begin{pmatrix} x^3+x^2+1 & 1 \\ x^2+1 & x^3+x+1 \end{pmatrix}$

- We then must mix the columns. This is computing E×M. E is a constant. $\begin{pmatrix} 1 & x^2 \\ x^2 & 1 \end{pmatrix} \times \begin{pmatrix} x^3+x^2+1 & 1 \\ x^2+1 & x^3+x+1 \end{pmatrix}$.

- We then get $\begin{pmatrix} (x^3+x^2+1)+(x^4+x^2) & 1+x^5+x^3+x^2 \\ (x^5+x^4+x^2)+(x^2+1) & x^2+x^3+x+1 \end{pmatrix}$

- To make it easier on ourselves we cancel like terms: $\begin{pmatrix} x^4+x^3+1 & x^5+x^3+x^2+1 \\ x^5+x^4+1 & x^3+x^2+x+1 \end{pmatrix}$ Since this problem is in $^4+x+1$,we divide each element by mod: $\begin{pmatrix} x^3+x & x^3+x+1 \\ x^2 & x^3+x^2+x+1 \end{pmatrix}$

- We then must convert our first key to polynomials and then add to our previous result: $\begin{pmatrix} x^3+x & x^3+x+1 \\ x^2 & x^3+x^2+x+1 \end{pmatrix} + \begin{pmatrix} x^3+x^2+x & x^3+x^2 \\ x^2+x+1 & 1 \end{pmatrix} = \begin{pmatrix} x^2 & x^2+x+1 \\ x+1 & x^3+x^2+x \end{pmatrix}$

- We then covert the polynomials back to bits and get a cipher of: $\begin{pmatrix} 0100 & 0111 \\ 0011 & 1110 \end{pmatrix}$ After running this through the SBOX, we get $\begin{pmatrix} 1101 & 0101 \\ 1011 & 1111 \end{pmatrix}$

- We then shift rows again: $\begin{pmatrix} 1101 & 0101 \\ 1111 & 1011 \end{pmatrix}$

- We then must xor with our second round key: $\begin{pmatrix} 1101 & 0101 \\ 1111 & 1011 \end{pmatrix} + \begin{pmatrix} 1001 & 0101 \\ 1011 & 1010 \end{pmatrix} = \begin{pmatrix} 0100 & 0000 \\ 0100 & 0001 \end{pmatrix}$

- Finally, we get a CIPHERTEXT of: 0100 0100 0000 0001