MATH 314 Spring 2024 - Class Notes

Wednesday 2/28/2024

Kamari Norton

\begin{document}

In today's class, we covered irreducible polynomials, SAES and Sboxes. For each topic we completed several examples in order to comprehend.

Include detailed notes from the lecture or class activities. Format your notes nicely using latex such as

\ Example: If we want F_4 we know F_4 F_2^2 we need an irreducible polynomial of degree 2. Consider the polynomials: x^2 , x^2+1 , x^2+x , and x^2+x+1

So, what are the elements or possible remainders?

They would be every polynomial of degree smaller than 2 such as $0, 1, x, x+1$

Now lets look at the field tables for 2 operations addition and multiplication

\begin{array}{|c|c|c|c|c|}
\hline
+& 0 & 1 & x &

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

and

\begin{array}{|c|c|c|c|c|}
\hline
*& 0 & 1 & x &

$*$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

Generally, F_2k is the $remainders \pmod{irreduciblepolynomial}$ of degree k \begin{itemize}
-NIST put out a new call for proposals for new cryptographic standards in the 1990s called Rigndael(“rain doll”)

-NIST was renamed AES (Advanced Encryption System)

-All computations in AES happen in $F_256 = F_2^8 \pmod{x^8 + x^4 + x^3 + x + 1}$

SAES is the simplified version of AES

-For SAES, we’ll use F_16 instead $(F_16 = f_2^4) \pmod{x^4 + x + 1}$

-Regualar: 128 bit keys, plaintexts/ciphertexts 256 bits, 10 rounds

-Simplified: 16 bit keys, 16 bit plaintexts/ciphertexts, 2 rounds

Sbox for SAES

-takes in 4 bits and outputs 4 bits

-convert to F_16 F(X)

-compute inverse $F^-1(x) \pmod{x^4 + x + 1}$

-convert coefficients to a vector \end{enumerate}

Find Sbox output for 1100 (hint: treat bits as coefficients of polynomial) First $1x^3 + 1x^2 + 0x + 0$ so $F(x) = x^3 + x^2$

Now compute $F^-1 \pmod{x^4 + x + 1}$ using Euclidean’s Algorithm

So, $(x^4 + x + 1) = (x + 1)(x^3 + x^2) + (x^2 + x + 1)$

$(x^3 + x^2) = x(x^2 + x + 1) + x$

$(x^2+x+1)=(x+1)x+1

Now solve for each remainder

$1 = (x^2 + x + 1) + (x + 1)x$

$x = (x^3 + x^2) + x(x^2 + x + 1)$

$(x^2 + x + 1) = (x^4 + x + 1) + (x + 1)(x^3 + x^2)$

Lastly, substitute and combine like terms

$1 = (x^2 + x + 1) + (x + 1)((x^3 + x^2) + x(x^2 + x + 1))$

$= (x^2 + x + 1) + (x + 1)(x^3 + x^2) + (x^2 + x)(x^2 + x + 1)$

$= (x + 1)(x^3 + x^2) + (x^2 + x + 1)(x^2 + x + 1)$

$1 = (x + 1)(x^3 + x^2) + (x^2 + x + 1)((x^4 + x + 1) + (x + 1)(x^3 + x^2))$

$= (x + 1)(x^3 + x^2) + (x^2 + x + 1)(x^4 + x + 1) + (x^2 + x + 1)(x + 1)(x^3 + x)$

Note:$ (x^2+x+1)(x+1) = x^{3+x}2+x)+(x^2+x+1) = x^3+1$

Continuing, $1 = (x+1)(x^3+x^2) + (x^2+x+1)(x^4+x+1) + (x^3+1)(x^3+x)$

$1 = (x^2+x+1)(x^4+x+1) + (x^3+x)(x^3+x^2) \pmod{x^4+x+1}$

So, $1 \equiv (x^3+x)(x^3+x) \pmod{x^4+x+1}$

$(x^3+x^2)^-1 \equiv x^3+x$ where we have 1010

Converting back to vector form, $v = 1010$

\end{document}