EE 8372 CRYPTOGRAPHY & DATA SECURITY

Homework 4
13 February 2020

Professor Dunham
Due: 20 February 2020

Review Paar Text: Chapter 3 & 4.
Suggested Reading in Menezes, Oorschot and Vanstone: Chapter 2, section 4, 5, and 6 .

1. Find all the irreducible polynomials in $Z_2[x]$ of degree 5. Note that $Z_2[x]$ represents all finite degree polynomials in powers of x, that x^3+x+1 and x^3+x^2+1 all the of the irreducible polynomials of degree 3, and that x^4+x+1, x^4+x^3+1 and $x^4+x^3+x^2+x+1$ are all of the irreducible polynomials of degree 4.

2. Construct the finite field $Z_2[x]/\left(x^4+x+1\right)$ which is isomorphic to GF(2^4). Let α be a root of the primitive polynomial x^4+x+1. Develop a table showing the relationship between the multiplicative representation and the additive representation for each element of this finite field. *Hint:* Consider multiplying the additive representation of an element by x. This is equivalent to the multiplicative calculation $\alpha^k * \alpha = \alpha^{k+1}$. If the degree of the resultant polynomial is less than 4, this is the additive field representation. Otherwise the degree of the resultant polynomial is 4 and you will need to subtract (add) the polynomial x^4+x+1 to lower the degree to 3 or less.

3. Let $\mathbf{A}$ be a non-singular matrix over GF(2). Consider the affine transformation $f(\mathbf{b}) = \mathbf{A}\mathbf{b}+\mathbf{c}$ where $\mathbf{c} \neq \mathbf{0}$. Determine the inverse transformation and show that it is an affine transformation.

4. The following matrix over GF(2) is used in the SubBytes Transformation in the AES:

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

   Find the inverse matrix over GF(2). *Hint:* Observe that this is a circulant matrix – each row/column is a cyclic (end around) shift of the first row/column. It is well known that the inverse matrix is also a circulant matrix. Hence it suffices to solve for the first row/column of the inverse matrix. This yields 8 equations over GF(2) in 8 unknowns which are readily solved. Other matrix inversion techniques will also work provided that you perform integer only calculations and that you restrict the integer solution to GF(2).