

## Cryptology – F03 – Note 4

### Lecture, February 18

We finished chapter 2 in the textbook and began on chapter 3, covering section 3.5.1.

### Lecture, February 25

We will cover chapter 3 in the textbook, skipping most of the first four sections. The original specification (which can be found through the course's homepage) will be used as the basis for the description of AES. We will probably begin on chapter 5.

### Lecture, March 4

We will continue with chapter 5. Note that subsections 5.2.1 and 5.2.3 were covered in discussion sections earlier.

### Problems for Thursday, March 6

Note that section numbers referred to in these problems are in the Rijndahl specification, which you can find on the Web. For problems using Maple, it is fine if you use Mathematica instead.

1. In the original description of Rijndael, it says that  $x^4 + 1$  (which is used to create the matrix for the MixColumn operation) is not irreducible over  $GF(2^8)$ . What are its factors? Try the function `Factor` in Maple, using `mod 2`. Check that the `mod 2` makes a difference by also trying to factor it with `factor`.

Check that  $x^8 + x^4 + x^3 + x + 1$  is irreducible over  $GF(2)$ . Check the multiplication done in the example in section 2.1.2 using the `modpol` function in Maple.

Find the inverse of  $x^7 + x^5 + x^3 + 1$  modulo  $x^8 + x^4 + x^3 + x + 1$ . Try the function `powmod` using the exponent  $-1$ . Check that your answer is correct using `modpol`.

2. Why do you think  $x^4 + 1$  was used, rather than an irreducible polynomial? Why are there no problems that it is not irreducible?
3. Check that the definition given for the polynomial  $d(x)$  in section 2.2 is correct. In Maple, I found it useful to multiply the polynomials, use the right mouse button to find `collect` and `x`, and repeatedly add on appropriate multiples of  $x^4 + 1$ . There might be a better way, but I couldn't get the `modpol` function to do anything in this case.

Similarly, check that the polynomial  $d(x)$  used in `MixColumn` in section 4.2.3 is correct.

This problem is probably just about as easy to do by hand.

4. Find the inverse transformation for `ByteSub` in section 4.2.1. To find the inverse modulo 2 of the matrix, you can use the `Inverse` function in Maple. To create the matrix, you can use the function `Matrix` (in the `LinearAlgebra` package, so you have to type `with(LinearAlgebra);` first) and list the matrix row by row. For example, to create the matrix  $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ , you can type `A:=Matrix([[1,2],[3,4]]);`. To check the result, you can multiply two matrices,  $A$  and  $B$  using `C:=A.B;`. To reduce all the elements of the matrix modulo 2, you can use the `Map` function, for example as `Map(modp,C,2);`
5. Do problem 3.3 in the textbook.
6. Do problem 3.7 in the textbook.