Cryptology
Problems

To be discussed Wednesday, February 28, 2001.

The first 4 questions have to do with Rijndael and use Maple to help you understand it.

1. In the description of Rijndael, it says that $x^4 + 1$ 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 polyomial $d(x)$ 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 3.2 in the textbook.