

Cryptology – E16 – Lecture 5

Lecture, September 14

We covered section 11.2, including the proof of Lemma 2.3 and the birthday bound at the top of page 24.

Lecture, September 20

We will cover chapter 12, concentrating on sections 12.1 and 12.2, and maybe begin on chapter 13.

Lecture, September 26

We will finish chapter 13.

Problem session September 27

1. Let $\text{DES}(x, k)$ represent the encryption of plaintext x with key k using the DES cryptosystem. Suppose $y = \text{DES}(x, k)$ and $y' = \text{DES}(c(x), c(k))$, where $c(\cdot)$ denotes the bitwise complement of its argument. Prove that $y' = c(y)$. Note that this can be proved without looking at the structure of the S-boxes. (Problem 2.10 in CTP.)

2. The textbook says that says that $X^4 + 1$ (which is used to create the matrix for the MixColumn operation) is reducible over the field $GF(2^8)$. 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 $GF(2)$.

Multiply $(x^6 + x^4 + x^2 + x + 1)(x^7 + x + 1) \bmod x^8 + x^4 + x^3 + x + 1$. You might use 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`.

3. Why do you think $X^4 + 1$ was used, rather than an irreducible polynomial? Why are there no problems that it is not irreducible?
4. Check that the polynomial $c(X)$ using in `MixColumns` can be calculated using the matrix shown on page 253 of the textbook.
5. Find the inverse transformation for `SubBytes`. 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);` or `with(LinearAlgebra[Modular]);` first) and list the matrix row by row (or create a matrix using the menu to the left and changing some entries). 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;` (or `Multiply(2,A,B)`). If you did not use the modular multiply, to reduce all the elements of the matrix modulo 2, you can use the `Map` function, for example as `Map(modp,C,2);`.
6. Why doesn't the last round of AES have the `MixColumn` operation?
7. I may lecture at the end.