MATH 195: CRYPTOGRAPHY
HOMEWORK #10

Problem R1. *Let k be a finite field, $\#k = q$, and let $k[X]$ be the ring of polynomials with coefficients in k. For $f = \sum_{i=0}^{n} c_i X^i \in k[X]$ and $a \in k$, write $f(a)$ for the element $\sum_{i=0}^{n} c_i a^i$ of k.*

(a) *Let $b \in k$ and define $f = 1 - (X - b)^{q-1}$. Prove:*

$$f(a) = \begin{cases} 0, & a \in k, a \neq b; \\ 1, & a = b. \end{cases}$$

(b) *Prove that there are precisely q^q different maps $g : k \to k$ and that for each of them there is a unique polynomial $f \in k[X]$ of degree $< q$ such that for all $a \in k$ one has $g(a) = f(a)$.*

Problem R2. *Refer to the notation in the notes on the Rijndael cipher from Tuesday, April 2.*

(a) *Prove: $\tau_s^2 = \mathrm{id}_{\mathcal{S}}$ and $\tau_s^{-1} = \tau_s$ for all $s \in \mathcal{S}$.*
(b) *Prove $\sigma^4 = \mathrm{id}_{\mathcal{S}}$ and $\sigma^{-1} = \sigma^3$.*

Problem R3.

(a) *Prove: $\beta\sigma = \sigma\beta$ independently of the map $B : \mathbb{F}_{256} \to \mathbb{F}_{256}$ used to define β.*
(b) *Prove: $\mu\tau_s = \tau_{\mu(s)}\mu$ for all $s \in \mathcal{S}$ independently of the linear function $M : \mathbb{F}_{256}^4 \to \mathbb{F}_{256}^4$ used to define μ.*

Date: April 9, 2002.
R1, R2.