MAS 433 Assignment

Wang Xueou (087199E16)

October 1, 2011

Exercise 1. Solution:

I. Finite Field Arthmetics

1. **poly_mult.m** (function ab=poly_mult(a, b, mod_pol)): Performs the multiplication of two polynomials (a and b) in GF(2^8) using a third polynomial (mod_pol) for the modular reduction.

II. AES_128 Implementation

aes_demo.m	**aes_demo** demonstrates the use of the AES_128 package. The call to **aes_init** supplies the actual en- and decryption function (**cipher** and **inv_cipher**)with expanded key schedule w, the substitution tables **s_box** and **inv_s_box**, and the polynomial matrices **poly_mat** and **inv_poly_mat**. These quantities have to be generated only once and can used by any subsequent en- or decipher.