# Problem Session CMPE-553 “Cryptography and Network Security” 22.05.2018

Chapter 4. Finite Fields

4.16. For polynomial arithmetic with coefficients in Z10, perform the following calculations

a. (7x+2)-(x2+5)

b. (6x2+x+3)\*( 5x2+2)

4.17. Determine which of the following are reducible over GF(2)

a. x3+1

b. x3+ x2+1

c. x4+1

4.18. Determine the gcd of the following pairs of polynomials:

a. x3+ x2+1 and x2+ x+1 over GF(2) (Answer:1)

b. x3-x+1 and x2+1 over GF(3) (Answer:1)

c. x5+ x4+ x3-x2-x+1 and x3+ x2+x+1 over GF(3) (Answer:x+1)

d. x5+ 88x4+73 x3+83x2+51x+67 and x3+ 97x2+40x+38 over GF(101) (answer: x+78)

4.19. Determine the multiplicative inverse of x3+ x+1 in GF(24) with m(x)= x4+x+1 (answer: x2+1)

Chapter 5. AES

5.1. show that a(x)={03}x3+{01}x2+{01}x+{02} and b(x)={0b}x3+{0d}x2+{09}x+{0e} are multiplicative inverses mod(x4+1) where coefficients of the polynomials are from GF(28) with irreducible polynomial m(x)=x8+x4+x3+x+1.

5.2. a. what is {01}-1 in GF(28)

b. verify the entry for {01} in the S-box

5.3. Show the first eight words of the key expansion for a 128-bit key of all zeros

5.4. Given the plaintext {000102030405060708090a0b0c0d0e0f} and the key {01010101010101010101010101010101}

a. show the original contents of state displayed as 4x4 matrix

b. show the value of State after initial AddRoundKey

c. Show the value of State after SubBytes

d. Show the value of State after ShiftRows

e. Show the value of State after MixColumns

5.5. Show that x imod(x 4+1)=ximod4











