EECE 455/632 – Cryptography and Network Security

Assignment

CHAPTER 4

Exercise 1 [20 points]

Determine GCD (43890, 12456)

Exercise 2 [20 points]

Use the extended Euclidean algorithm to find the multiplicative inverse of:

a) 12345 mod 67890
b) 54321 mod 98765

Exercise 3 [20 points]

For polynomial arithmetic with coefficients in Z_{10}, perform the following calculations:

a) $(x^2 - 6x + 4) – (3x^2 + 7)$

b) $(8x^2 + 2x + 6) * (4x^2 + 3)$

Exercise 4 [20 points]

Determine the multiplicative inverse of $x^3 + x + 1$ in $GF(2^4)$,

with $m(x) = x^4 + x + 1$

Exercise 5 [20 points]

Show that an integer N is congruent modulo 9 to the sum of its decimal digits.

For example, $583 \equiv 5 + 8 + 3 = 16 \equiv 1 + 6 = 7 \bmod 9$.