CSE589, CSE/IT441 Cryptography & Applications – Fall 2017

Department of Computer Science, New Mexico Tech
Lecturer: Dongwan Shin

HOMEWORK 3 - Assigned: 10/25, **Due: 11/1** (*midnight*)[1]

Please **type your answers** and **submit** them to Canvas.

Problem 1. [**5 points**] Does the set of residue classes modulo 21 form a group

a. with respect to addition? (*Show why or why not*)
b. with respect to multiplication? (*Show why or why not*)

Problem 2. [**5 points**] Consider the set $S = \{a, b\}$ with addition and multiplication defined by the following tables:

+	a	b
a	b	a
b	a	b

x	a	b
a	b	b
b	b	a

Is S a ring? Justify your answer.

Problem 3. [**5 points**] Determine which of the following are reducible over GF(2):

a. $x^4 + 1$
b. $x^6 + x^2 + 1$
c. $x^5 + 1$

Problem 4. [**5 points**] Prove the following:

a. [(a *mod* n) - (b *mod* n)] *mod* n = (a - b) *mod* n
b. [(a *mod* n) x (b *mod* n)] *mod* n = (a x b) *mod* n

Problem 5. [**10 points**] This problem provides a numerical example of a portion of AES encryption. Please refer to AES S-boxes and MixColumns matrix in your textbook in order to solve this problem. Given a plaintext and a key as follows,

`The Plaintext:`
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

`The Key:`
10 11 10 11 10 11 10 11 10 11 10 11 10 11 10 11

a. Show the original contents of **State**, displayed as a 4 × 4 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.

[1]Except for Programming Lab, which is due on 11/10 (Friday). The solution for the programming lab should be submitted by email (**dongwan.shin@nmt.edu**).

Programming Lab 1. [**100 points**] This lab is to conduct a linear cryptanalysis attack to find the key used to encrypt messages.

The cipher used for encryption is the basic Substitution-Permutation Network (SPN) you implemented for the 2nd homework, with the following S-Box used instead.

Table 1: S-Box Representation

input	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
output	2	C	4	1	7	A	B	6	8	5	3	F	D	0	E	9

A number of pairs of plaintext and ciphertext are provided in the attached **knownpairs.txt** file. Referring to *A Tutorial on Linear and Differential Cryptanalysis* by *Howard M. Heys*, answer the following:

a. [**20 points**] Provide a linear approximation table similar to Table 4.
b. [**30 points**] Discuss your linear approximation approach for the complete cipher, as in Section 3.4.
c. [**40 points**] Provide a table for your experimental result for linear attack similar to Table 5.
c. [**10 points**] What is the key used for encryption?