Math 259: Spring 2019
Quiz 5

NAME:

Are you taking this class for graduate credit?

Time: **30 minutes**

Problem	Value	Score
1	4	
2	3	
3	7	
4	6	
TOTAL	20	

Problem 1 : (4 points) Let

$$\begin{aligned} F\colon \mathbb{F}_2^4 &\to \mathbb{F}_2^3 \\ x &\mapsto (f_1(x), f_2(x), f_3(x)) \end{aligned}$$

be a public key given by the quadratic polynomials

$$\begin{aligned} f_1(x_1, x_2, x_3, x_4) &= x_1x_2 + x_2x_3 + x_1 + x_4, \\ f_2(x_1, x_2, x_3, x_4) &= x_2x_4 + x_3x_4 + x_1 + x_2 + x_3, \\ f_3(x_1, x_2, x_3, x_4) &= x_1x_3 + x_2x_3 + x_3x_4 + 1. \end{aligned}$$

Is

$$x = (1, 0, 1, 1)$$

a valid signature for the message digest

$$y = (0, 1, 1)?$$

Please justify your answer with some computations and a short sentence.

Problem 2 : (3 points) This problem presents a series of statements. For each, please indicate if the statement is true or false.

The question will be graded in such a way as to reward **self-consistency** over correctness. In other words, you can earn a point for answering a question in a manner consistent with your previous answers, even if it is wrong. You can also lose a point for answering a question in a manner inconsistent with your previous answers, even if it is right.

a) In an "oil and vinegar" multivariate polynomial, "oil" variables may be multiplied together but "vinegar" variables may not.

b) The following system of multivariate quadratic polynomials is an oil and vinegar system, with x_1 and x_2 "oil" variables and x_3 and x_4 "vinegar" variables:

$$\begin{aligned} P\colon \mathbb{F}_2^4 &\to \mathbb{F}_2^2 \\ x &\mapsto (p_1(x), p_2(x)), \end{aligned}$$

where

$$\begin{aligned} p_1(x_1, x_2, x_3, x_4) &= x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4 + x_2, \\ p_2(x_1, x_2, x_3, x_4) &= x_1x_3 + x_2x_4 + x_3x_4 + x_3 + 1. \end{aligned}$$

c) To solve an oil and vinegar system where x_1 and x_2 are "oil" variables and x_3 and x_4 are"vinegar" variables, you should first fix random values of x_1 and x_2. This will give you a linear system in x_3 and x_4 which can then be solved using linear algebra (if a solution exists).

Problem 3 : (7 points) Let β be a root of the irreducible polynomial $f(x) = x^2 + x + 1$ over $\mathbb{F}_2$. According to the theory we have developed in class, this means that $\mathbb{F}_4 = \mathbb{F}_2[\beta]$.

a) (4 points) Write down a multiplication table for $\mathbb{F}_2[\beta]$.

This is still part of the same problem, where β is a root of $f(x) = x^2 + x + 1$ and $\mathbb{F}_4 = \mathbb{F}_2[\beta]$.

b) (3 points) Compute the following quantities:

i. β^{-1}

ii. β^4

iii. $(\beta + 1)^5$

Problem 4 : (6 points) Consider the HFE polynomial

$$G(X) = X^9 \in \mathbb{F}_4[X].$$

Give the associated multivariate quadratic polynomial $G\colon (\mathbb{F}_2)^2 \to (\mathbb{F}_2)^2$. Throughout, use the field structure $\mathbb{F}_4 = \mathbb{F}_2[\beta]$, where β is a root of $x^2 + x + 1$.