Home Assignment 3 - B1
EITN41

Joel Pålsson & Rasmus Olofzon

December 5, 2017

1 Algorithms

This is our algorithm for Binding:

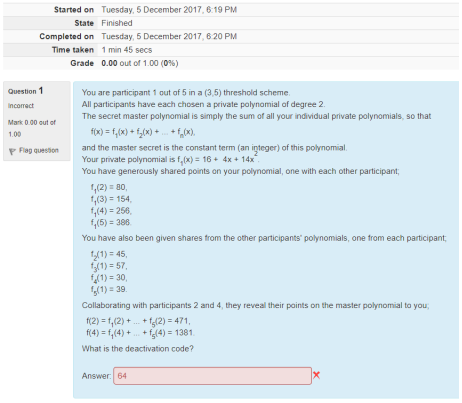
$$1 + 1 \neq 3$$

This is our algorithm for Concealing:

$$1 + 1 \equiv 3$$

2 Results

2.1 Binding



Started on	Tuesday, 5 December 2017, 6:19 PM
State	Finished
Completed on	Tuesday, 5 December 2017, 6:20 PM
Time taken	1 min 45 secs
Grade	**0.00** out of 1.00 (**0%**)

Question 1

Incorrect

Mark 0.00 out of 1.00

Flag question

You are participant 1 out of 5 in a (3,5) threshold scheme.
All participants have each chosen a private polynomial of degree 2.
The secret master polynomial is simply the sum of all your individual private polynomials, so that

$f(x) = f_1(x) + f_2(x) + \ldots + f_5(x)$,

and the master secret is the constant term (an integer) of this polynomial.
Your private polynomial is $f_1(x) = 16 + 4x + 14x^2$.
You have generously shared points on your polynomial, one with each other participant;

$f_1(2) = 80$,
$f_1(3) = 164$,
$f_1(4) = 256$,
$f_1(5) = 386$.

You have also been given shares from the other participants' polynomials, one from each participant;

$f_2(1) = 45$,
$f_3(1) = 57$,
$f_4(1) = 30$,
$f_5(1) = 39$.

Collaborating with participants 2 and 4, they reveal their points on the master polynomial to you;

$f(2) = f_1(2) + \ldots + f_5(2) = 471$,
$f(4) = f_1(4) + \ldots + f_5(4) = 1381$.

What is the deactivation code?

Answer: 64

2.2 Concealing

Started on	Tuesday, 5 December 2017, 6:19 PM
State	Finished
Completed on	Tuesday, 5 December 2017, 6:20 PM
Time taken	1 min 45 secs
Grade	**0.00** out of 1.00 (**0%**)

Question 1

Incorrect

Mark 0.00 out of 1.00

Flag question

You are participant 1 out of 5 in a (3,5) threshold scheme

All participants have each chosen a private polynomial of degree 2.

The secret master polynomial is simply the sum of all your individual private polynomials, so that

$f(x) = f_1(x) + f_2(x) + \ldots + f_5(x)$.

and the master secret is the constant term (an integer) of this polynomial

Your private polynomial is $f_1(x) = 16 + 4x + 1x^2$

You have generously shared points on your polynomial, one with each other participant:

$f_1(2) = 80$,
$f_1(3) = 154$,
$f_1(4) = 256$,
$f_1(5) = 388$.

You have also been given shares from the other participants' polynomials, one from each participant:

$f_2(1) = 45$,
$f_3(1) = 57$,
$f_4(1) = 30$,
$f_5(1) = 39$.

Collaborating with participants 2 and 4, they reveal their points on the master polynomial to you:

$f(2) = f_1(2) + \ldots + f_5(2) = 417$,
$f(4) = f_1(4) + \ldots + f_5(4) = 1381$.

What is the deactivation code?

Answer: 64