Solutions to CNS Exercises

Exercise 1

SECRET SHARING - BASIC EXAMPLE

Assume a (3,5) Secret Sharing scheme, with standard numbering of parties. i.e., $P_i \rightarrow x_i = \{1,2,3,4,5\}$. Using arithmetic modulus 11, the dealer hides a secret S in the range [0,10]. At reconstruction time, Parties 1,2 and 4 show their shares:

P1 → share1 = 4

P2 → share2 = 7

P4 → share4 = 9

What is the secret?

Solution:

Remembering the general formula for the Lagrange Coefficient in the (**t,n**) case: $A_i = \prod_{k \neq i} \frac{-x_k}{x_i - x_k}$ having 3 out of 5 shares the secret is completely revealed and is computable through the means of the above formula as follows:

$$A_1 = \prod_{k \neq 1} \frac{-x_k}{x_1 - x_k} = \left(\frac{-2}{1-2}\right)\left(\frac{-4}{1-4}\right) = \frac{8}{3} \qquad A_4 = \prod_{k \neq 4} \frac{-x_k}{x_4 - x_k} = \left(\frac{-1}{4-1}\right)\left(\frac{-2}{4-2}\right) = \frac{1}{3}$$

$$A_2 = \prod_{k \neq 2} \frac{-x_k}{x_2 - x_k} = \left(\frac{-1}{2-1}\right)\left(\frac{-4}{2-4}\right) = -2$$

Now we can compute the secret as:

$S = 4\left(\frac{8}{3}\right) + 7(-2) + 9\left(\frac{1}{3}\right) \ mod\ 11$

Remark: Multiplicative inverse mod n

$\frac{1}{3} = 3^{-1} \text{mod } 11 = ?$ we need to find $x \ \ s.t.$

$$3x = 1\ mod 11$$

in this case is 4: $3 \cdot 4 = 12\ mod\ 11 = 1$

So the Solution can be written as follows:

$S = 4 \cdot 8 \cdot 4 + 7(-2) + 9 \cdot 4 \ \ mod\ 11 = 128 - 14 + 36 = 150\ mod 11 = 7$ ■

Exercise 2

2: SECRET SHARING – Information leakage

Assume the same SS scheme as in exercise 1 above but in this case using **ordinary arithmetic – NO MODULUS**! The dealt secret S was the range [0,10]. At reconstruction time, Parties 2 and 4 show their shares:

P2 → share2 = 29

P4 → share4 = 75

Prove that even if a third share is missing, this information is sufficient to completely reveal the secret!

[*hint: write an expression parametric in the hidden secret S, and show that only one value in the range [0,10] satisfies a condition…*]

Solution:

In this case we have only 2 out of 5 shares so we need to use a trick in order to guess, in this case completely reveal, the secret. Let's calculate as before shares for x = 1, 2 ,4

$$A_1 = \prod_{k\neq 1} \frac{-x_k}{x_1 - x_k} = \left(\frac{-2}{1-2}\right)\left(\frac{-4}{1-4}\right) = \frac{8}{3} \qquad A_4 = \prod_{k\neq 4} \frac{-x_k}{x_4 - x_k} = \left(\frac{-1}{4-1}\right)\left(\frac{-2}{4-2}\right) = \frac{1}{3}$$

$$A_2 = \prod_{k\neq 2} \frac{-x_k}{x_2 - x_k} = \left(\frac{-1}{2-1}\right)\left(\frac{-4}{2-4}\right) = -2$$

Now we can't derive the secret because the share bind to x=1 is not known BUT we know something else about the solution: the share **must be** an integer value, so let's write out the parametric function as hinted by the professor.

$$S = x\left(\frac{8}{3}\right) + 29(-2) + 75\left(\frac{1}{3}\right) = x\left(\frac{8}{3}\right) - 33 \xrightarrow{yields} x = \frac{3(S+33)}{8}$$

Now given $S \in (1, \dots, 10)$ we can guess until we find a value of S that yields an integer value for x

- S = 1
  $x = \frac{3(1+33)}{8} = \frac{102}{8}$ *not integer*
- S = 2
  $x = \frac{3(2+33)}{8} = \frac{105}{8}$ *not integer*
- S = 3
  $x = \frac{3(3+33)}{8} = \frac{108}{8}$ *not integer*
- S = 4
  $x = \frac{3(4+33)}{8} = \frac{111}{8}$ *not integer*
- S = 5
  $x = \frac{3(5+33)}{8} = \frac{114}{8}$ *not integer*
- S = 6
  $x = \frac{3(6+33)}{8} = \frac{117}{8}$ *not integer*
- S = 7
  $x = \frac{3(7+33)}{8} = \frac{120}{8} = 15$ *valid share*
- S = 8
  $x = \frac{3(8+33)}{8} = \frac{123}{8}$ *not integer*
- S = 9
  $x = \frac{3(9+33)}{8} = \frac{126}{8}$ *not integer*
- S = 10
  $x = \frac{3(10+33)}{8} = \frac{129}{8}$ *not intege*

Given the educated guess we've made, the secret is 7 because, in this case, is the only result which leads to an integer share value. ■

Exercise 3

3: Common Modulus Attack

An RSA scheme uses modulus n = 77; A same message M is RSA-encrypted using two different public keys e1 = 17 and e2 = 23, but same modulus n=77. The two resulting ciphertexts are: c1=60 and c2=53. Decrypt the message applying the Common Modulus Attack.

Solution:

We have:

$c_1 = M^{e_1} = 60\ with\ e_1 = 17$

$c_2 = M^{e_2} = 53\ with\ e_2 = 23$

$\gcd(17,23) = 1$

Our goal is to find x and y s. t. $17x + 23y = 1\ mod\ n$ because we would have decrypted the message without knowing anything else about it as: $M^{e_1 x + e_2 y} = M\ mod\ n$

In order to find such number, we need to find the Bézout identity and a way is to use the extended Euclidian algorithm as follows:

Euclidean Algorithm	**Highlighting the reminders**
$23 = 17 * (1) + 6$	$6 = 23 - 17 * (1)$
$17 = 6 * (2) + 5$	$5 = 17 - 6 * (2)$
$6 = 5 * (1) + 1$	$1 = 6 - 5 * (1)$
$5 = 5 * (1) + 0$	

After having highlighted the reminders we can collapse all the equation inside the last one obtaining, as we'd imagine the gcd(17,23) expressed in terms of those two numbers:

$$1 = 3(23) - 4(17)$$

$$x = -4, \qquad y = 3$$

Now we only have to just compute:

$M^{e_1 x + e_2 y} = (60^{-4} \cdot 53^3)\ mod\ n = 37$ ■

Exercise 4

4: verifiable Secret Sharing

Let p=83 and q=(p-1)/2 = 41.

Assume a (2,n) Verifiable Secret Sharing scheme with Modulus 41 which uses the Feldmann scheme with g=10 and modulus 83. The commitments are:

C0 = 23

C1 = 4

Party P7 (x=7) receives share s7 = 29: verify that this is a valid share.

Solution:

Having the initial commitments, computing it for x = 7 is immediate:

$$c_0 = g^s \; and \; c_1 = g^{a_1} \rightarrow g^{p(x)} = g^{s+x \cdot a_1}$$

$$c_7 = g^{s+7 \cdot a_1} = c_0 \cdot c_1^7 = 23 \cdot 4^7 \; mod \; p = \mathbf{12}$$

We can now verify it against the supposed shares received: $g^{29} mod \; p = 10^{29} \; mod \; p = \mathbf{12}$ ■

Exercise 5

5: Find elliptic Curve Points

Consider the Elliptic curve

$$y^2 = x^3 + 2x + 1$$

defined over the modular integer field Z_5:

find all the points EC(Z_5)

Solution

Given any point that lies in an EC it induce a subgroup on the elliptic curve, we can compute all elliptic curve points as sums of a given point.

Let P = (0,1) clearly it lies on the EC, we can now sum it to itself to obtain [2]P that would be another point.

- [2]P = $(x_2, y_2) = (1,3)$
  - $\lambda_2 = \frac{3x_1+a}{2y_1} = \frac{2}{2} \; mod \; 5 = 1 \; mod \; 5$
  - $x_2 = \lambda_2^2 - 2x_1 = 1 \; mod \; 5$
  - $y_2 = \lambda_2(x_1 - x_2) - y_1 = 1(0-1) - 1 = -2 \; mod \; 5 = 3 \; mod \; 5$

- [3]P = [2]P + P = (1,3) + (0,1) = $(x_3, y_3) = (3,3)$
  - $\lambda_3 = \frac{y_2 - y_1}{x_2 - x_1} = 2 \; mod \; 5$
  - $x_3 = \lambda_3^2 - x_2 - x_3 = 3 \; mod \; 5$
  - $y_3 = \lambda_3(x_2 - x_3) - y_2 = 2(1-3) - 3 = -7 \; mod \; 5 = 3 \; mod \; 5$

- [4]P = $(x_4, y_4) = (3,2)$
  - $\lambda_4 = \frac{y_3 - y_2}{x_3 - x_2} = \frac{2}{3} \; mod \; 5 = 4 \; mod \; 5$
  - $x_4 = \lambda_4^2 - x_3 - x_2 = 3 \; mod \; 5$
  - $y_4 = \lambda_4(x_3 - x_4) - y_3 = 4(3-3) - 3 = -3 \; mod \; 5 = 2 \; mod \; 5$

- [5]P = $(x_5, y_5) = (1,2)$
  - $\lambda_5 = \frac{y_4 - y_3}{x_4 - x_3} = \frac{1}{3} \; mod \; 5 = 2 \; mod \; 5$
  - $x_5 = \lambda_5^2 - x_4 - x_3 = 1 \; mod \; 5$
  - $y_5 = \lambda(x_4 - x_5) - y_4 = 2(3-1) - 2 = 2 \; mod \; 5$

- [6]P = $(x_6, y_6) = (0,4)$
  - $\lambda_6 = \frac{y_5 - y_4}{x_5 - x_4} = 1 \; mod \; 5$
  - $x_6 = \lambda_6^2 - x_5 - x_4 = 0 \; mod \; 5$
  - $y_6 = \lambda(x_5 - x_6) - y_5 = 1(1-0) - 2 = -1 \; mod \; 5 = 4 \; mod \; 5$

After this point futher sums leads to point that doesn't lies on the EC, or restart the cycle. So all the point found so far, lies on the EC and are the only points that the EC generates.

Another possible method would be to check if all the point (= the pairs given by [0,4]X[0,4]) does or does not lies on the EC ■

Notes on the Quadratic Residues

It does exist another method to calculate the cardinality of the EC and all of its point that relies on the quadratic residues mod n as follows:

In number theory, an integer q is called a ***quadratic residue modulo n***[1] *if it is congruent to a perfect square modulo n; i.e., if there exists an integer x such that:*

$$x^2 \equiv q \ (mod\ n)$$

Otherwise, q is called a quadratic ***nonresidue*** *modulo n.*

In order to calculate all points we can do as follows:

Let E be the curve defined as above: $y^2 = x^3 + 2x + 1 \bmod 5$
Let's write a simple table were we populate $\forall\ x \in [0,5]$ their quadratic residues mod 5

Now, solving the above equation for x_i means find $y\ s.t.\ y^2 = x_i^3 + 2x_i + 1\ mod\ 5$
But having now filled the table of possible quadratic residues y^2 has to be equal to one or more terms in the x column.

x	$x^2\ mod\ 5$
0	0
1	1
2	4
3	4
4	1

In order to be more precise and clear we now create a table summing up all the information so far gathered, and we will see that it would be much simpler now to find all possible points.

x	$x^2\ mod\ 5$	$y^2 = x^3 + 2x + 1$	**Points**
0	0	1	(0,1),(04)
1	1	4	(1,2),(1,3)
2	4	3	-
3	4	4	(3,2),(3,3)
4	1	3	-

The last column is populated like this: ($x_i, x_j\ s.t.\ y_i^2\ mod\ 5 = x_j^2\ mod\ 5$) indeed when $\boldsymbol{y^2 = 3}$ there is no $\boldsymbol{x_j}$ s. t. $\boldsymbol{x_j^2 = 3\ mod\ 5}$■

[1] https://en.wikipedia.org/wiki/Quadratic_residues

Exercise 6

6: Pairing Based crypto

Being e: GxG→Gt a bilinear map, and g a generator of G, simplify the expression:

$e(g^x \times g^y, g^z)^w / e(g^{wz}, g^x)$

Solution:

Given all the hypothesis we can rewrite it like this:

$$\frac{e(g^x \cdot g^y, g^z)^w}{e(g,g)^{xwz}} = \frac{\hat{g}^{(x+y)wz}}{\hat{g}^{xwz}} = \hat{g}^{(x-x+y)wz} = \hat{g}^{ywz} \blacksquare$$