Tutorial 6 (TA. John Ehab)

(t,n)-Secret Sharing:

N is the total number of secret shareholders

T is our threshold, t or more parties can re-construct the secret, t-1 parties have zero info about the secret

Shamir's Secret Sharing:

t = k ➡ polynomial of degree k-1
example: an equation for a line (degree 1), can be constructed using at least 2 points (t=2)

Each secret share is just a point (x,y)

The secret itself is the y-intercept; x = 0

To construct the equation P(x) "that'll be used to find the secret later when substituting x with 0" from given points "shares", we use Lagrange Interpolation.

Lagrange Interpolation:

- P(x) if (2,n):

$$P(x) = y_1 \cdot \frac{x - x_2}{x_1 - x_2} + y_2 \cdot \frac{x - x_1}{x_2 - x_1}$$

(or simply Y = m . X + c
m is the slope "(y2-y1) / (x2-x1)"
➡ substitute with any point to get c)

- P(x) if (3,n):

$$P(x) = y_1 \cdot \frac{(x - x_2)(x - x_3)}{(x_1 - x_2)(x_1 - x_3)} + y_2 \cdot \frac{(x - x_1)(x - x_3)}{(x_2 - x_1)(x_2 - x_3)} + y_3 \cdot \frac{(x - x_1)(x - x_2)}{(x_3 - x_1)(x_3 - x_2)}$$

Exercise 6–2:

To find the final result, don't forget our modulus 😁

53 / 8 is not division, it's 53 % 17 * 8^{-1} % 17

a= 17 b= 8

Calculate! 😀

Output

This is the output of the **Extended Euclidean Algorithm** using the numbers a=**17** and b=**8**:

a	b	q	r	s1	s2	s3	t1	t2	t3
17	8	2	1	1	0	1	0	1	-2
8	1	8	0	0	1	-8	1	-2	17

➔ 53 / 8 (mod 17) = 2 * (-2%17) = 2 * 15 = 30 % 17 = 13

Exercise 6-3:

Same "division under the modulo" concept when finding the results of the slopes

AB = 3 / 2 mod 11 = 3 * 6 = 18 % 11 = 7

AC = -3 / 4 mod 11 = 8 * 3 = 24 % 11 = 2

AD = -2 / 6 mod 11 = 9 * 2 = 18 % 11 = 7