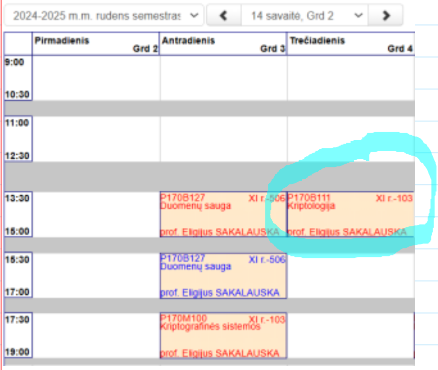
111_012 Secret-Sharing-Sch

Those who do not want to avoid oral answering to the Mid-Term Exam (MTE) questions are graded by 7.

The requirements of Poster Report are presented in:
https://docs.google.com/document/d/1raqTudLCNlLm3wLFCDp_V7QnOg_EFH6d/edit?usp=sharing&ouid=111502255533491874828&rtpof=true&sd=true

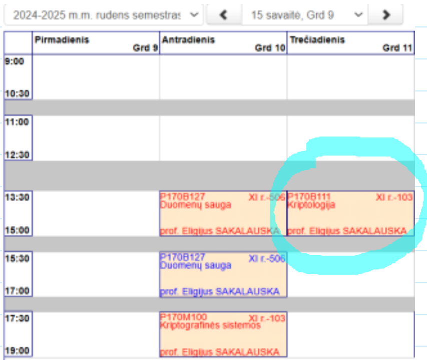
The list of topics is presented in:
https://docs.google.com/document/d/1B6gavCsgZXcCRssFZEWLVfzaO_IPbC5o/edit?usp=sharing&ouid=111502255533491874828&rtpof=true&sd=true

Poster Report presentation (37 students)



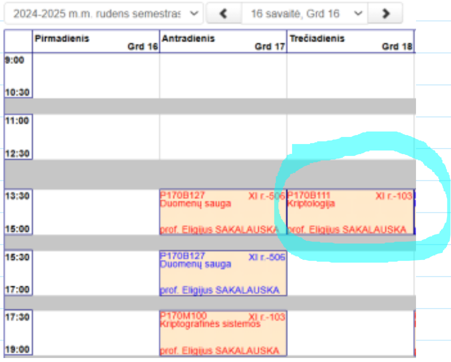
2024-2025 m.m. rudens semestras | 14 savaitė, Grd 2

	Pirmadienis Grd 2	Antradienis Grd 3	Trečiadienis Grd 4
9:00 10:30			
11:00 12:30			
13:30 15:00		P170B127 XI r.-506 Duomenų sauga prof. Eligijus SAKALAUSKA	P170B111 XI r.-103 Kriptologija prof. Eligijus SAKALAUSKA
15:30 17:00		P170B127 XI r.-506 Duomenų sauga prof. Eligijus SAKALAUSKA	
17:30 19:00		P170M100 XI r.-103 Kriptografinės sistemos prof. Eligijus SAKALAUSKA	



2024-2025 m.m. rudens semestras | 15 savaitė, Grd 9

	Pirmadienis Grd 9	Antradienis Grd 10	Trečiadienis Grd 11
9:00 10:30			
11:00 12:30			
13:30 15:00		P170B127 XI r.-506 Duomenų sauga prof. Eligijus SAKALAUSKA	P170B111 XI r.-103 Kriptologija prof. Eligijus SAKALAUSKA
15:30 17:00		P170B127 XI r.-506 Duomenų sauga prof. Eligijus SAKALAUSKA	
17:30 19:00		P170M100 XI r.-103 Kriptografinės sistemos prof. Eligijus SAKALAUSKA	



2024-2025 m.m. rudens semestras | 16 savaitė, Grd 16

	Pirmadienis Grd 16	Antradienis Grd 17	Trečiadienis Grd 18
9:00 10:30			
11:00 12:30			
13:30 15:00		P170B127 XI r.-506 Duomenų sauga prof. Eligijus SAKALAUSKA	P170B111 XI r.-103 Kriptologija prof. Eligijus SAKALAUSKA
15:30 17:00		P170B127 XI r.-506 Duomenų sauga prof. Eligijus SAKALAUSKA	
17:30 19:00		P170M100 XI r.-103 Kriptografinės sistemos prof. Eligijus SAKALAUSKA	

Cookery recipe

Secret Sharing scheme

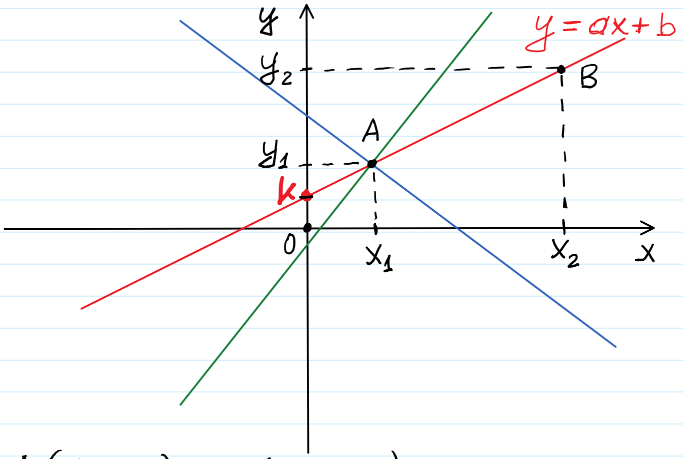
Shamir's Secret Sharing (SSS) is used to secure a secret in a distributed way, most often to secure other encryption keys. The secret is split into multiple parts, called **shares**. These shares are used to reconstruct the original secret.
To unlock the secret via Shamir's secret sharing, a minimum number of shares are needed. This is called the **threshold**, and is used to denote the minimum number of shares needed to unlock the secret. An adversary who discovers any number of shares less than the threshold will not have any additional information about the secured secret-- this is called perfect secrecy. In this sense, SSS is a generalisation of the one-time pad - Vernam cipher (which is effectively SSS with a two-share threshold and two shares in total).
Let us walk through an example:
Problem: Company XYZ needs to secure their vault's passcode. They could use something standard, such as AES, but what if the holder of the key is unavailable or dies? What if the key is compromised via a malicious hacker or the holder of the key turns rogue, and uses their power over the vault to their benefit?
This is where SSS comes in. It can be used to encrypt the vault's passcode and generate a certain number of shares, where a certain number of shares can be allocated to each executive within Company XYZ. Now, only if they pool their shares can they unlock the vault. The threshold can be appropriately set for the number of executives, so the vault is always able to be accessed by the authorized individuals. Should a share or two fall into the wrong hands, they couldn't open the passcode unless the other executives cooperated.
From <https://en.wikipedia.org/wiki/Shamir%27s_Secret_Sharing>

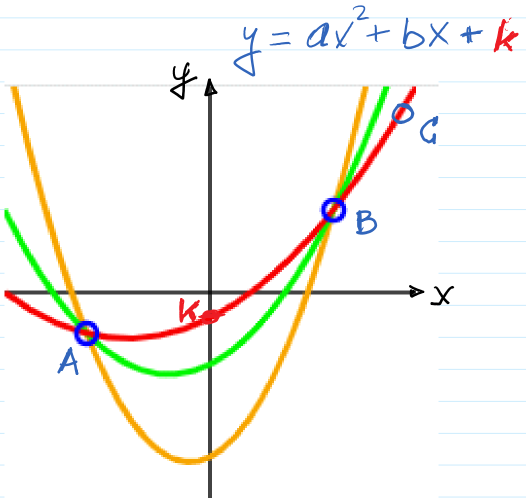
Shamir's Secret Sharing is an ideal and perfect (***t***, ***N***)-**threshold** scheme.
In such a scheme, the aim is to divide a secret ***k*** which is a ***secret key*** to decrypt a receipt
Is divided into ***N*** pieces of data ***P1***, ***P2***, ..., ***PN*** known as **shares** in such a way that:

1. Knowledge of any ***t*** or more ***P$_i$*** pieces makes ***k*** easily computable. Therefore ***t*** is is named as **threshold** . That is, the complete secret ***k*** can be reconstructed from any combination of ***t*** or more pieces of data.
2. Knowledge of any ***t***-1 or fewer ***P$_i$*** pieces leaves ***k*** completely undetermined, in the sense that the possible values for ***k*** seem as likely as with knowledge of **0** pieces. The secret ***k*** cannot be reconstructed with fewer than ***t*** pieces.

If ***t=N***, then every piece of the original secret is required to reconstruct the secret.

We are considering the field of real numbers $\langle R, +, -, *, : \rangle$.
Then the plain consisting of real numbers is $R^2 = \{(x,y);\ x \in R, y \in R\}$





$A(x_1, y_1);\ B(x_2, y_2).$

$$-\begin{cases} a x_1 + b = y_1 \\ a x_2 + b = y_2 \end{cases}$$

$$a(x_1 - x_2) = y_1 - y_2 \Rightarrow a = \frac{y_1 - y_2}{x_1 - x_2}$$

$$b = y(x=0) = (ax + b)\Big|_{x=0}$$

$$b = k$$

One can draw an infinite number of polynomials of degree 2 through 2 points. 3 points are required to define a unique polynomial of degree 2. This image is for illustration purposes only — Shamir's scheme uses polynomials over a finite field.

From <https://en.wikipedia.org/wiki/Shamir%27s_Secret_Sharing>

$$y = ax^2 + bx + k$$

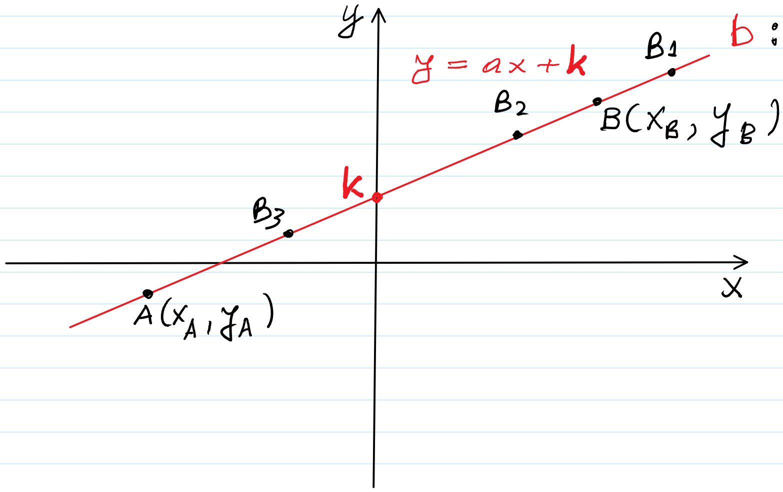
$A(x_1, y_1);\ B(x_2, y_2);\ C(x_3, y_3)$

By solving this linear system of equation, parabola coefficients a, b, k can be obtained. $\Leftarrow$

$$\begin{cases} a x_1^2 + b x_1 + c = y_1 \\ a x_2^2 + b x_2 + c = y_2 \\ a x_3^2 + b x_3 + c = y_3 \end{cases}$$

of equation, parabola coefficients $\Longleftarrow \begin{cases} a x_2^2 + b x_2 + c = y_2 \\ a x_3^2 + b x_3 + c = y_3 \end{cases}$

a, b, k can be obtained.



b: $Enc_k(Rec) = C$; $Rec = Dec_k(C)$

Rec : secret recipe

$Enc(k, Rec) = C_{Rec}$

$Dec(k, C_{Rec}) = Rec$

shares: $\{A, B, B_1, B_2, B_3\}$

In the case of linear interpolation Threshold=2

If (A, B) can not participate in recovery secret k, then secret k can be recovered by any other pair $(B_1, B_2), (B_1, B_3), (B_2, B_3)$

In general, secret k can be recovered by C_5^2 pairs

$(A, B), (A, B_1), (A, B_2), \ldots, (B_2, B_3)$ $\quad C_5^2 = \frac{5 \cdot 4}{2} = 10$

But 2-shares could be not enough to protect the secret k. due to bribering ....

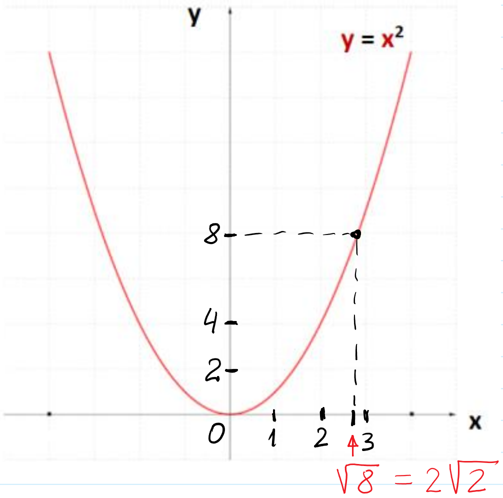
Let it be 3-share created to protect the secret.

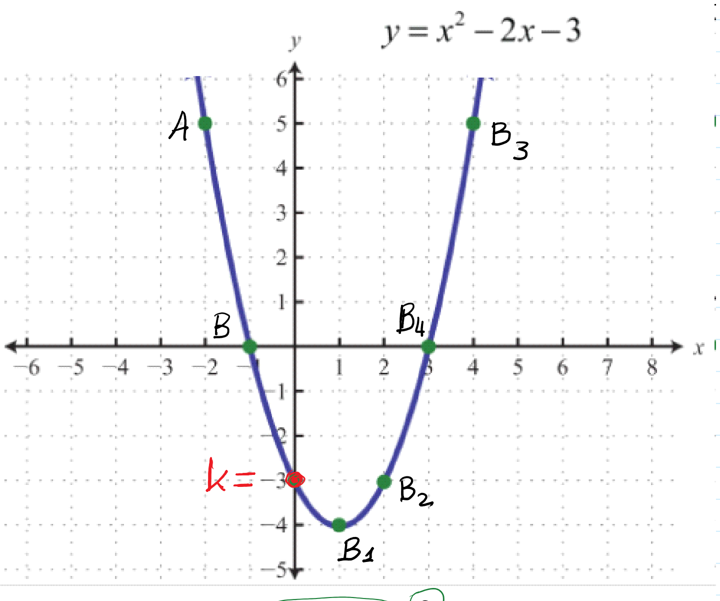
It is required to choose parabola $y = ax + bx + k$ whic can be recovered by Lagrangian interpolation using 3-points $(A, B, C) \Longrightarrow$ threshold $= 3$

A decided to share the secret to 6-parts among $\{A, B, B_1, B_2, B_3, B_4\}$

The number of triplets to recover secret k is

$$C_6^3 = \frac{\cancel{6} \cdot 5 \cdot 4}{\cancel{3 \cdot 2} \cdot 1} = 20.$$





$$\begin{cases} a x_1^2 + b x_1 + k = y_1 \\ a x_2^2 + b x_2 + k = y_2 \\ a x_3^2 + b x_3 + k = y_3 \end{cases} \quad t = 3$$

$$\boxed{n} = t - 1 = 3 - 1 = \boxed{2.}$$

$$y = a x^{\boxed{2}} + bx + k$$

$$k = -3$$

For any $t = n+1$ we must choose n-th degree polynomial

$$y = p_n(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x^1 + a_0; \quad a_0 = k.$$

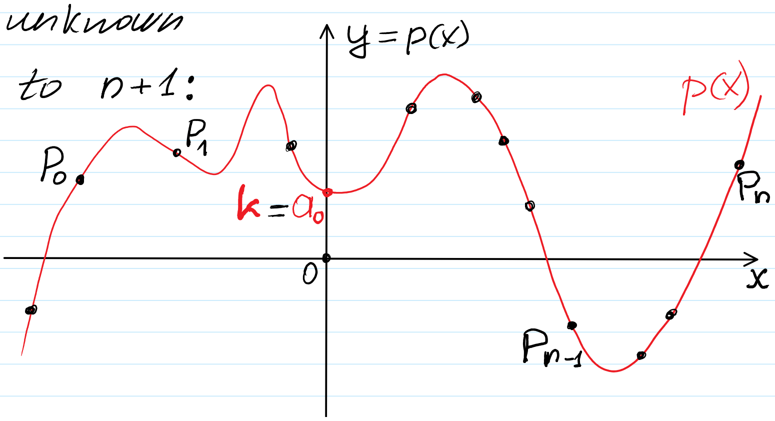
This polynomial can be recovered by Lagrange interpolation technique having $n+1$ points - uniquely recovered!

$$\{ P_1, P_2, \dots, P_{n+1}] \longleftarrow \{ (x_1, y_1), (x_2, y_2), \dots, (x_{n+1}, y_{n+1})$$

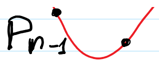
$$\left.\begin{cases} a_n x_1^n + a_{n-1} x_1^{n-1} + \dots + a_0 = y_1 \\ - - - - - - - - - - - - - - \\ a_n x_{n+1}^n + a_{n-1} x_{n+1}^{n-1} + \dots + a_0 = y_{n+1} \end{cases}\right\} \Rightarrow (a_n, a_{n-1}, \dots, a_1, \underset{\substack{\downarrow \\ k}}{a_0})$$

Let $p(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ be a polynomial of order n.

In $p(x)$ the number of unknown coefficients is equal to $n+1$: to define $p(x)$ it is required to construct $n+1$ linear equations to find coefficients $\{a_0, a_1, \dots, a_{n-1}, a_n\}$.



to find coefficients
$\{a_0, a_1, \dots, a_{n-1}, a_n\}$.
We must have $(n+1)$ points
$\{P_0, P_1, \dots, P_{n-1}, P_n\}$
where $p(x)$ is crossing
these poits.



This technique is named Lagrangian interpolation: $t-1=n$.

$$k = a_0 = p(x=0) = \sum_{i=0}^{t-1} y_i \prod_{\substack{j=0 \\ i\neq j}}^{t-1} \frac{x_j}{x_j - x_i}$$

Infinite field R must be replaced by finite field $F_p = \mathcal{Z}_p$.

Arithmetic of Finite fields $\mathbf{Z}_p = \mathbf{F}_p = \{0, 1, 2, \dots, p-1\}$, when **p** is prime.

+ mod **p**, - mod **p**, * mod **p**, : mod **p**   : mod p by „0": $z/0$ - is not defined.

1) $\mathcal{Z}_p$ in an additive group: $\langle \mathcal{Z}_p, + \bmod p \rangle$
2) $\mathcal{Z}_p$ has multiplicative group $\mathcal{Z}_p^* = \{1, 2, 3, \dots, p-1\}$
$\mathcal{Z}_p^* \subset \mathcal{Z}_p$ $\langle \mathcal{Z}_p^*, * \bmod p \rangle$
3) The distributive law takes place in $\mathcal{Z}_p$:
for all $a, b, c \in \mathcal{Z}_p$: $a*(b+c) = (a*b + a*c) \bmod p$

$$\prod_{i=1}^{3} a_i = a_1 \circ a_2 \circ a_3$$

$\mathcal{Z}_{11} = \{0, 1, 2, \dots, 10\}$: $+, -, \bullet, :$ mod 11

Till this place