EPITECH. TECHNOLOGY

103cipher

B-MAT-100

Cryptography

- Securing communication between two parties, to prevent a third party to access it.
- Examples:
  - Caesar cipher
  - Enigma machine
  - RSA

Example: Caesar cipher

- Key = number
- Shift alphabet by the key
- Substitue each letter of the message by the corresponding letter in the new alphabet

Example: Caesar cipher

Example:

- Key = 7

ABCDEFGHIJKLMNOPQRSTUVWXYZ → HIJKLMNOPQRSTUVWXYZABCDEFG

- Input: « AVE CAESAR, MORITURI TE SALUTANT »
- Output: « HCL JHLZHY, TVYPABYP AL ZHSBAHUA »

103cipher

- Implementing the Hill cipher
- Inputs
  - Message
  - Key
  - Flag (0 to encrypt, 1 to decrypt)
- Outputs
  - Key Matrix
  - Encrypted/Decrypted message
- Using a matrix calculus library is considered cheating

Encryption

- Convert key into the smallest square matrix K

"abcdefg" → 97, 98, 99, 100, 101, 102, 103 → $\mathrm{K} = \begin{pmatrix} 97 & 98 & 99 \\ 100 & 101 & 102 \\ 103 & 0 & 0 \end{pmatrix}$

- Convert the message into a matrix M with the same number of columns as K (fill with zeros if needed).
- Compute the encrypted matrix $M' = M.K$.
- Display M' as a list of numbers.

Decryption

- Convert key into the smallest square matrix K
- Compute K^{-1} (the inverse of K).
- Convert the encrypted message into a matrix M' with the same number of columns as K.
- Compute the decrypted matrix $M = M'.K^{-1}$.
- Display M as a list of numbers.

Matrices

EPITECH. TECHNOLOGY

- Two-dimensional array of values

$$\begin{pmatrix} 42 & 12 & 34 & 2 \\ 36 & 2 & 1 & 15 \\ 3 & 23 & 17 & 9 \end{pmatrix}$$

Multiplication of two matrices

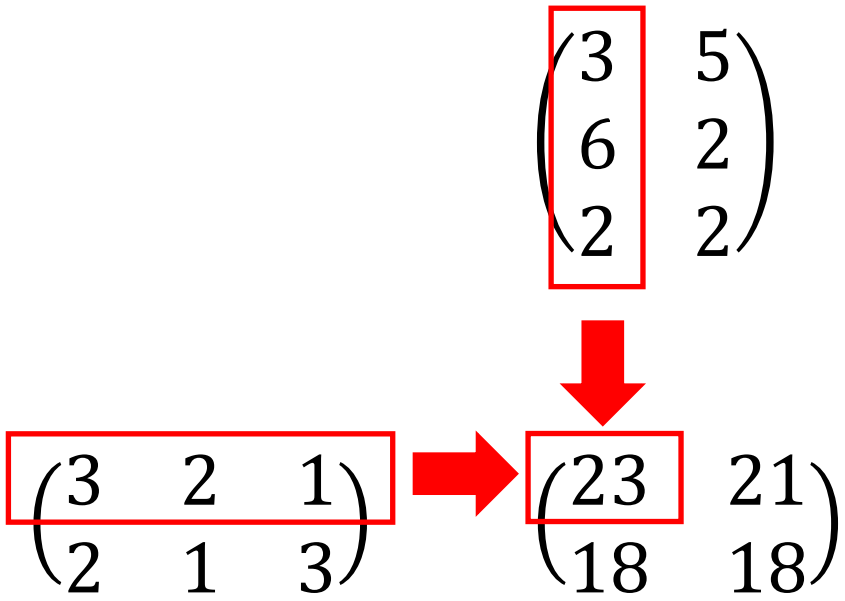
EPITECH. TECHNOLOGY

- Two matrices can be multiplied if the number of columns of the first one is the same as the number of rows of the second one

$$\begin{pmatrix} 3 & 2 & 1 \\ 2 & 1 & 3 \end{pmatrix} * \begin{pmatrix} 3 & 5 \\ 6 & 2 \\ 2 & 2 \end{pmatrix} = \begin{pmatrix} 23 & 21 \\ 18 & 18 \end{pmatrix}$$

- The resulting matrix has the number of rows of the first one and the number of columns of the second one
- The multiplication is not commutative! A*B ≠ B*A

How to multiply matrices



$$(3 * 3) + (2 * 6) + (1 * 2) = 9 + 12 + 2 = 23$$

Transpose of a matrix

EPITECH. TECHNOLOGY

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}$$

$$A^T = \begin{pmatrix} a_{11} & \cdots & a_{m1} \\ \vdots & \ddots & \vdots \\ a_{1n} & \cdots & a_{mn} \end{pmatrix}$$

$$A = \begin{pmatrix} 3 & 4 & 1 \\ 2 & 1 & 3 \end{pmatrix} \qquad A^T = \begin{pmatrix} 3 & 2 \\ 4 & 1 \\ 1 & 3 \end{pmatrix}$$

Identity matrix

$$I = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

If A is a square matrix with the same dimensions as I:

$$A.I = I.A = A$$

Inverse of a matrix

EPITECH. TECHNOLOGY

- If A is a square matrix, B is the inverse of A if:

$$A.B = B.A = I$$

- We denote A^{-1} the inverse of A.

- A matrix is inversible if $\det(A) \neq 0$.
- $\det(A)$ is the determinant of A.

Inverse of a 1x1 matrix

$$A = (a)$$

$$\det(A) = a$$

$$if\ \det(A) \neq 0\text{: } A^{-1} = \left(\frac{1}{a}\right)$$

Inverse of a 2x2 matrix

EPITECH. TECHNOLOGY

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

$$\det(A) = \begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - cb \neq 0 \, ?$$

$$A^{-1} = \frac{1}{\det(A)} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

What about higher dimensions ?

- Formula based on cofactors (cf. Bootstrap…)

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$$

$$A_{11} = (-1)^{1+1} \begin{vmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{vmatrix}$$

- For this project, you only have to inverse up to 3x3.

Suggested boni

- Inverse of matrices larger than 3x3
- Decrypt without the key
- Improve the encryption process