Part I
Crypting

This matrix encryption algorithm is based on the LU factorization, the resolution of which will be recalled by Gaussian elimination.

Horner recursive basic construction schemes and signed cyclic permutations will also be used.

Let the matrix M to be encrypted be defined by

$$M = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \\ 3 & 4 & 1 & 2 \\ 4 & 1 & 2 & 3 \end{bmatrix}$$

We start by evaluating the size of M and adjusting with a default value if necessary in order to obtain a square matrix (An LU factorization is only possible on a square matrix.).

We will distinguish 4 matrices per image, respectively the matrices with values Red, Blue, Green and Alpha.

The progress of the algorithm being identical, one will generalize it to the resolution of the encryption of the matrix M.

Once the size has been adjusted if necessary, we first carry out an LU factorization of M.

Factorization

Based on the following properties :

- Any lower matrix resulting from an LU factorization has a diagonal made up of 1
- Any multiplication of a lower matrix and an upper matrix resulting from an LU factorization does not admit as one and only result the original matrix

We will factorize the matrix M and adapt the matrices L and U to the algorithm using the Gauss elimination:

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \\ 3 & 4 & 1 & 2 \\ 4 & 1 & 2 & 3 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 2 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 & 4 \\ 0 & -1 & -2 & -7 \\ 3 & 4 & 1 & 2 \\ 4 & 1 & 2 & 3 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 2 & 1 & 0 & 0 \\ 3 & 0 & 1 & 0 \\ 4 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 & 4 \\ 0 & -1 & -2 & -7 \\ 0 & -2 & -8 & -10 \\ 0 & -7 & -10 & -13 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 2 & 1 & 0 & 0 \\ 3 & 2 & 1 & 0 \\ 4 & 7 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 & 4 \\ 0 & -1 & -2 & -7 \\ 0 & 0 & -4 & 4 \\ 0 & 0 & 4 & 36 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 2 & 1 & 0 & 0 \\ 3 & 2 & 1 & 0 \\ 4 & 7 & -1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 & 4 \\ 0 & -1 & -2 & -7 \\ 0 & 0 & -4 & 4 \\ 0 & 0 & 0 & 40 \end{bmatrix}$$

Let the matrices L and U be obtained by the factorization LU of the matrix M

$$L = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 2 & 1 & 0 & 0 \\ 3 & 2 & 1 & 0 \\ 4 & 7 & -1 & 1 \end{bmatrix} U = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 0 & -1 & -2 & -7 \\ 0 & 0 & -4 & 4 \\ 0 & 0 & 0 & 40 \end{bmatrix}$$

We will adapt L to the algorithm by subtracting the identity matrix I_4 from it.

$$\text{L'=L-}I_4\text{=} \begin{bmatrix} 0 & 0 & 0 & 0 \\ 2 & 0 & 0 & 0 \\ 3 & 2 & 0 & 0 \\ 4 & 7 & -1 & 0 \end{bmatrix}$$

Once the matrices L 'and U have been calculated, we will add them into the numbered matrix C defined by:

$$\text{C=L'+U=} \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & -1 & -2 & -7 \\ 3 & 2 & -4 & 4 \\ 4 & 7 & -1 & 40 \end{bmatrix}$$

This encrypted matrix C will be called an "intermediate encryption matrix".

Once the matrix C has been optimized for the algorithm, we will perform a signed σ permutation such that

$$size(M) \quad modulo \quad size(\sigma) = 0$$

$\Longrightarrow$ Here, $size(M) = size(\sigma) = 4$

Let the signed permutation σ defined on the columns of C with signature :

$$\sigma = [3, 1, 0, 2]$$

Signed permutation

The permutation is defined by the following property: to each σ signed permutation we can associate its M_σ permutation matrix.

Here, for $\sigma = [3, 1, 0, 2]$,

$$M_\sigma = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix}$$

$$\boxed{\sigma(C) = C.M_\sigma}$$

$$\sigma(C) = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & -1 & -2 & -7 \\ 3 & 2 & -4 & 4 \\ 4 & 7 & -1 & 40 \end{bmatrix} \cdot \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 4 & 2 & 1 & 3 \\ -7 & -1 & 2 & -2 \\ 4 & 2 & 3 & -4 \\ 40 & 7 & 4 & -1 \end{bmatrix}$$

$$C' = \sigma(C) = \begin{bmatrix} 4 & 2 & 1 & 3 \\ -7 & -1 & 2 & -2 \\ 4 & 2 & 3 & -4 \\ 40 & 7 & 4 & -1 \end{bmatrix}$$

The reverse permutation σ^{-1} will be calculated by transposing the matrix M_σ

$$\Longrightarrow \boxed{\begin{aligned} C &= \sigma^{-1}(\sigma(C)) \\ &= \sigma^{-1}(C.M_\sigma) \\ &= C.M_\sigma.{}^tM_\sigma \\ &= C.I_d \\ &= C \end{aligned}}$$

Bases Transposition

Once the matrix has been transposed, we will use the permutation signature defined by

$$\sigma = [2, 1, 3, 0]$$

as the key of the algorithm. The key ξ is defined by the relation

$$\boxed{\xi_i = \sigma_i + 11}$$

$\Longrightarrow Here, \xi = [13, 12, 14, 11]$

We will calculate the table of associated bases as an example, for what follows we will refer to a table of complete bases.
Either the base conversion application *phi* defined by:

$$\boxed{\varphi : C_{i,j} \longrightarrow C'_{i,j} = (C_{i,j})_{\xi_i}}$$

Where ξ_i determine the associated digital base.
In order to make the encryption more complex, we will multiply the matrix C by a coefficient α.

Here, we will choose $\alpha = 100$ arbitrarily. The higher α, the more complex the encryption. Let us calculate C 'the encrypted matrix to be transmitted where :

$$\boxed{C' = \varphi(\alpha.C) = \begin{bmatrix} 24a & 125 & 79 & 1a1 \\ -4a4 & -84 & 148 & -148 \\ 208 & 104 & 176 & -208 \\ 3007 & 587 & 334 & -91 \end{bmatrix}}$$

The associated matrix $M(\xi)$ is

$$M(\xi) = \begin{bmatrix} 13 & 13 & 13 & 13 \\ 12 & 12 & 12 & 12 \\ 14 & 14 & 14 & 14 \\ 11 & 11 & 11 & 11 \end{bmatrix}$$

Give us the key as the first column :

$$\boxed{\xi = [13, 12, 14, 11]}$$

Part II
Decrypting

Inverse Bases Transposition

Let the matrix C 'to be decrypted associated with the encryption key xi, both defined by

$$C' = \begin{bmatrix} 24a & 125 & 79 & 1a1 \\ -4a4 & -84 & 148 & -148 \\ 208 & 104 & 176 & -208 \\ 3007 & 587 & 334 & -91 \end{bmatrix}$$

$$\xi = [13, 12, 14, 11]$$

From ξ we will extract σ by inverse mapping :

$$\Longrightarrow \boxed{\sigma_i = \xi_i - 11}$$

$$\Longleftrightarrow \boxed{\sigma = [2, 1, 3, 0]}$$

With C 'we will associate the application θ such that

$$\theta = \varphi^{-1}$$
$$\Longleftrightarrow \theta(\varphi(C)) = C$$
$$\Longleftrightarrow \theta(C') = C$$

With

$$\begin{cases} (C'_{i,j})_{\xi_i} \longrightarrow (C_{i,j})_{10} \\ Base(\xi_i) \longrightarrow Base(10) \end{cases}.$$

Let's compute $D = \theta(C')$

$$D = \begin{bmatrix} 400 & 200 & 100 & 300 \\ -700 & -100 & 200 & -200 \\ 400 & 200 & 300 & -400 \\ 4000 & 700 & 400 & -100 \end{bmatrix}$$

We go to divide the matrix D by the Constant coefficient α previously fixed.

$$\frac{D}{\alpha} = \begin{bmatrix} 4 & 2 & 1 & 3 \\ -7 & -1 & 2 & -2 \\ 4 & 2 & 3 & -4 \\ 4 & 7 & 4 & -1 \end{bmatrix}$$

Inverse Signed permutation

On va calculer la permutation cyclique signée τ telle que

$$\tau = \sigma^{-1} \Longrightarrow M(\tau) = M(\sigma_{-1}) =^t M(\sigma)$$
$$= \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

In order to find the original matrix, we will multiply

$$\frac{D}{\alpha}.M(\tau) \Longrightarrow \boxed{C = \frac{D}{\alpha}.M(\tau)}$$

$$C = \begin{bmatrix} 4 & 2 & 1 & 3 \\ -7 & -1 & 2 & -2 \\ 4 & 2 & 3 & -4 \\ 4 & 7 & 4 & -1 \end{bmatrix} . \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & -1 & -2 & -7 \\ 3 & 2 & -4 & 4 \\ 4 & 7 & -1 & 40 \end{bmatrix}$$

We have found the ciphered matrix C by successive algebraic operations which we will convert into matrices L and U by the following system:

$$\begin{cases} L = inferior\_triangle(C) - diagonal(C) + Id_4 \\ U = upper\_triangle(C) \end{cases}$$

We will place the diagonal of C on U by convention

Multiplication

So let

$$L = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 2 & 0 & 0 & 0 \\ 3 & 2 & 0 & 0 \\ 4 & 7 & -1 & 0 \end{bmatrix} + \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 2 & 1 & 0 & 0 \\ 3 & 2 & 1 & 0 \\ 4 & 7 & -1 & 1 \end{bmatrix}$$

$$U = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 0 & -1 & -2 & -7 \\ 0 & 0 & -4 & 4 \\ 0 & 0 & 0 & 40 \end{bmatrix}$$

We restore the matrix M decrypted by the following operation: $M = L.U$

$$M = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 2 & 1 & 0 & 0 \\ 3 & 2 & 1 & 0 \\ 4 & 7 & -1 & 1 \end{bmatrix} + \begin{bmatrix} 1 & 2 & 3 & 4 \\ 0 & -1 & -2 & -7 \\ 0 & 0 & -4 & 4 \\ 0 & 0 & 0 & 40 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \\ 3 & 4 & 1 & 2 \\ 4 & 1 & 2 & 3 \end{bmatrix}$$

Finally

$$\boxed{M = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \\ 3 & 4 & 1 & 2 \\ 4 & 1 & 2 & 3 \end{bmatrix}}$$

$\Longrightarrow$ The matrix M is found, the encryption application is reversible and injective, that is to say that it admits only one antecedent.

$\Longrightarrow$ The algorithm is valid