**Data Security and Cryptology Final Project**

**Secure access to dataset of image files.**

**Password access to the data. An image must be encrypted/decrypted by Mars in CFB mode; secure channel for secret key delivery with EC El-Gamal + RSA digital signature using SHA-256.**

Group members:

Liran Hersh – 203955299

Noy Maman – 313594434

Karin Azulay – 316541549

Asaf Darmon – 205404080

The project study process:

\*Learn how to encrypt and decrypt an image by Mars in CFB mode (how it works, its structure and understanding the implementation).

To work with Mars algorithm, we needed to divide the image matrix into 128-bit blocks and generate 128-bit to 448-bit key for encryption and decryption.

\*Learn about Symmetric keys and how it works.

\*Learn about how to get Secure access for delivery key for dataset of image files.

\*Learn about Elliptic Curves (how it works, its structure and implementation).

\*Learn how to **encrypt using** El Gamal algorithm.

\* Learn Digital signature using RSA with SHA-256 and how it helps us in our project.

**The project flow:**

At first, we took a picture, made a division into 128-bit blocks each (Mars algorithm knows how to work only with 128-bit size blocks).

Each block was encrypted by Mars algorithm.

Note that we encrypted and decrypted each block with Mars algorithm using CFB mode.

Next, we took the Mars key (in which we generate earlier), encrypted it with the help of El-Gamal elliptical curve and Alice private key.

Then we made a digital signature with SHA-256 using RSA algorithm.

At final stage, we sent bob the encrypted image and Alice's signature.

**The obtained results**:

We managed to get to a point where there is secure access to blocks of image files. We divide each block to fit Mars so Image can be encrypted / decrypted using Mars in CFB mode.

We wanted to reach a situation where we have a secure channel for secret key delivery using EC El-Gamal algorithm.

In addition, we wanted to sign 'Mars' key so no one would be able interfere between Bob and Alice. We sign 'Mars' key using RSA algorithm with SHA-256.

**Conclusions:**

We create Secure access to image file. Password access to the data. Our image was encrypted and decrypted using Mars algorithm in CFB mode.

We deliver the encrypted Mars key securely to Bob Using El Gamal and sign the image using RSA algorithm with SHA-256.