Shahar Berenson 208608414  
Shlomi Fridman 318187002  
Omer Goldstein 205906258

Data Security and Cryptology

Summary Report

## Process of the project study

We’ve received the project assignment of “Secure email exchange” between two users, and the algorithms to be used:

* Blowfish
* McEliece
* ECDSA

We began by reading about the algorithms and searching for Python implementations of them to be used in the practical section of the project.

Afterwards, we began to compile the presentation while working parallelly on the Python implementation of the project.

## Project Flow

The project flow involved weekly meetings. We met online and discussed the assignment, then worked towards completing the presentation and the report.  
Furthermore, meetings with the lecturers (Renata and Zeev) occurred to discuss the direction of the project and get clarifications.

## Motivation

### Why Blowfish?

Its fast encryption after setup and free availability make it ideal for encrypting the actual email message contents. While the key setup is expensive, this is acceptable in our scenario where the same key is reused for a session.

### Why McEliece?

It is resistant to quantum attacks, unlike RSA or ECC, due to the NP-hardness of decoding a linear code. Although it has a large public key size, its efficiency and future-proof security make it an excellent choice for key encapsulation in a secure email system.

### Why ECDSA?

ECDSA is chosen for its short key size and high security per bit, making it efficient for signing emails and ideal for environments with limited computational resources.

## Results

1. A Python script that simulates email exchange with secure encryption and a digital signature between two users (Alice and Bob).
2. A presentation on the 3 given algorithms with an explanation on each, detailed steps, and known attacks to guard against.

## Conclusion

This project presents a comprehensive and robust solution for secure email exchange by integrating three cryptographic mechanisms, each chosen for its strengths:

* Blowfish for fast, secure content encryption.
* McEliece for quantum-resistant key encapsulation.
* ECDSA for strong digital signatures.

Together, they provide confidentiality, integrity, and authenticity, making the system both secure and practical for real-world deployment.

Links

[Github](https://github.com/ShlomiFridman/CryptoProject2025/)

[Google Colab notebook](https://colab.research.google.com/drive/1kMEcHvLSnAOkE__pteiKiFjM3FB59UQJ?usp=sharing)

[Blowfish implementation](https://github.com/ananya2407/Blowfish-Algorithm)

[McEliece Implementation](https://github.com/elibtronic/pythonMCS)  
[ECDSA Implementation](https://dev.to/exemak/bitcoin-signatures-from-scratch-44-ecdsa-implementation-in-python-using-zero-dependencies-410c)