Project Report

An Application for secure email exchange: including encryption-decryption with

AES-CFB and signature based on EL-GAMAL on elliptic curve.

SECTION A: Project profile

|  |  |
| --- | --- |
| **Project title:** | Secure Email Application |
| **Project members:** | Kfir Gaon, Roman Ratchitski, Shoval Yehuda, Rafael Mosheyoff  Group 29 |
| **Project tools:** | Python,Html5,Css,Javascript,Sqlite |
| **Project security:** | AES,CFB,ECC,EL-GAMAL |

SECTION B: Project report and reflection

1. **Project description:** The project main objective is to simulate an email application where users can send messages between them base on a TCP/IP network communication in a secure way using Symmetrical Encryption and Asymmetrical Encryption as AES with CFB mode and El-GAMAL with ECC.
2. **Process of the project study:** We took a week to learn and improve the knowledge on the given algorithms then we made 3 appointments a week on zoom and spoke about the subject and ideas to how implement base on what we learned till that point then we meet on the Haifa university together to distribute the application code taking in count which algorithm each member of the group will speak about in the presentation. we chose to use python as the main language because its easy to handle and fast to implement our algorithms hence we could to provide a GUI interface using web technologies, we studied from the following sources:

* Lectures, Information Security and Cryptology
* Practices, Information Security and Cryptology
* National Institute of Standards and Technology , AES [(click)](https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf)
* Wikipedia Block cipher mode of operation , CFB [(click)](https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation)
* Daniel R. L. Brown, SEC Elliptic Curves [(click)](http://www.secg.org/sec2-v2.pdf)
* Prof Bill Buchanan OBE, El-Gamal and ECC [(click)](https://medium.com/asecuritysite-when-bob-met-alice/elgamal-and-elliptic-curve-cryptography-ecc-8b72c3c3555e)

1. **Project flow**: The project uses a simple GUI interface using Html, Css, Javascript using flask

as framework on python allowing the user to stablish a connecting with the server via TCP/IP network communication.

* Every user has email, password, private key, public key the last two are generated by our signature key class and all his details are store in the Sqlite database.
* The user login to the server with his email and password the server gets the request and verify the information.
* The user sends email, the sent email is encrypted with AES-CFB then the sender user ask for the receive user public key from server, Then with the public key using EL-GAMAL with ECC the AES key is encrypted then is email is stored in the database with the following details (from,to,cypher\_email,c1,c2,iv,date).
* The user gets his income emails by making a request to receive his private key from server then requests his email list that is stored in the database, the user receives a list of encrypted emails - (from,to,cypher\_email,c1,c2,iv,date)

using his private key the user decrypt the AES key using EL-GAMAL with ECC then with the AES key and iv the user decrypt the cypther\_email using AES-CFB this process repeats his self for each email in the list.

1. **Project results:** The results were as we expected the messages are encrypted with a

Symmetrical Encryption (AES-CFB) and the AES key is encrypted with an Asymmetrical Encryption (EL-GAMAL-ECC) and the result is store in the database creating an unreadable and total secured message for anyone that does not match the digital signature of the receiver.

1. **Project conclusion:** The combination of encryption methods has various advantages as

Asymmetric encryption can slow down the encryption process because the calculates are more complex, but with the simultaneous use of symmetric encryption and encrypting the symmetric key with the asymmetric encryption creating a faster and secure connecting between the users.