Group 22 | Project Report

An Application for secure e-mail exchange encryption-decryption with LEA cipher in CBC mode, including secure delivery of the secret key with EC EL-GAMAL + Rabin

Maryanne Halabi 206537458

Dana Asulin 206027534

Amit Ben David 205818883

Sapir Dayan 313605776

Project description:

The project’s main objective is to send encrypted e-mail with digital signature, so the receiver can be sure that the decrypted e-mail is the original.

The Lea algorithm protects the text in Cbc mode, the secret key is delivered with EL-GAMAL algorithm and Rabin digital signature ensures the source validation.

**Project flow:**

We have used Spyder intelligent development environment and Python language to implement and execute our project.

Now, we will explain the flow of our project :

Bob wants to send an encrypted message to Alice: Bob picks a prime number, we mark it as: P, picks a primitive number that is smaller then P,it’s the generator of p we mark it as: g, and picks a natural number we mark it as: a.

Bob calculates : = A

Bob sends the public key A and also send g,p.

Alice received the public key,g,and p and She selects a one-time random K number and then she calculates:

) ,

Alice - signs the encrypted key with the help of a Rabin digital signature and then sends it to Bob (m is the encrypted key).

Bob checks that Alice is the signer and decrypt the encrypted key m using :

Bob discovers the original key.

Then divides the original text he wants to encrypt into 128-bit blocks. For block 1 he performs XOR with initial vector IV and thenshe performs encryption of the block using the LEA algorithm with the key that was found.

Then, on the next original block it performs XOR with the previous encrypted block, and on it he performs LEA encryption using the key and so on.

Finally, he gets encrypted blocks - and merges them into encrypted text.

he sends them to Alice, and Alice will decrypt the encrypted text by decryption with LEA using the key she sent, and with CBC.

And in the end of the process Alice will discover the original text email.

**Project results:**

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated