**Data Security and Cryptology**

**An application for secure access to database on two levels: to read and to edit. Encryption/Decryption by Salsa20 cipher, secret key delivery with McEliece cryptosystem + ECDSA**

Name: \*\*\*\* ID: \*\*\*\*\*\*\*\*\*

Name: \*\*\*\* ID: \*\*\*\*\*\*\*\*\*

Name: \*\*\*\* ID: \*\*\*\*\*\*\*\*\*

Name: Dvir Bublil ID: \*\*\*\*\*\*\*\*\*

**The project study process:**

At first, we met to coordinate expectations, and agree on a way of working throughout the project. After that we were required to research and understand in depth the algorithms that we must implement and use in our project. After the individual learning, we met again as a group, to share the knowledge, that we acquired, because of that meeting, we understood the algorithms in a broader and deeper way, and in addition we planned a common language regarding the work to be done in the project. During this meeting, many questions arose, some of the questions were resolved by the team members, but there were also questions which we could not find an answer, so we asked one of the lecturers of the course to understand the material in the best possible way. After we had no more questions about the algorithms, we met again to start working on the presentation, and the code of the project. While researching the subject we found half implementations of the algorithms across the internet on various platforms. And so, we had to understand how to combine and connect them to achieve the realization necessary for our project. When we worked on the code, we used tools that allow us to work at the same time, such as Git and GitHub, and almost always throughout the project we worked as a group, except in exceptional cases, in which we divided the work among the team members.

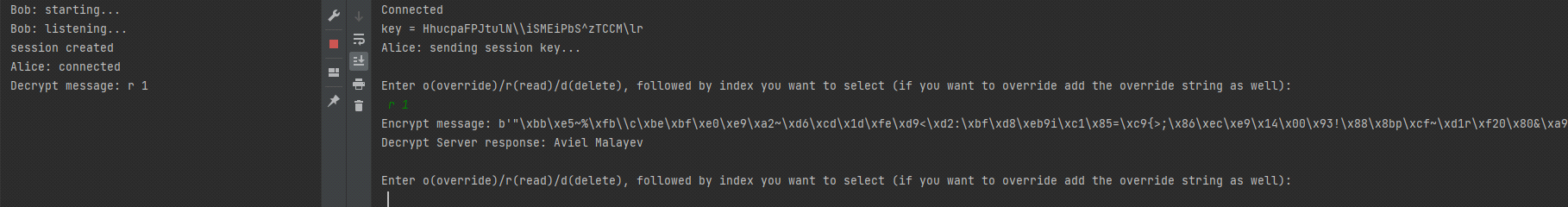
**The project flow:**

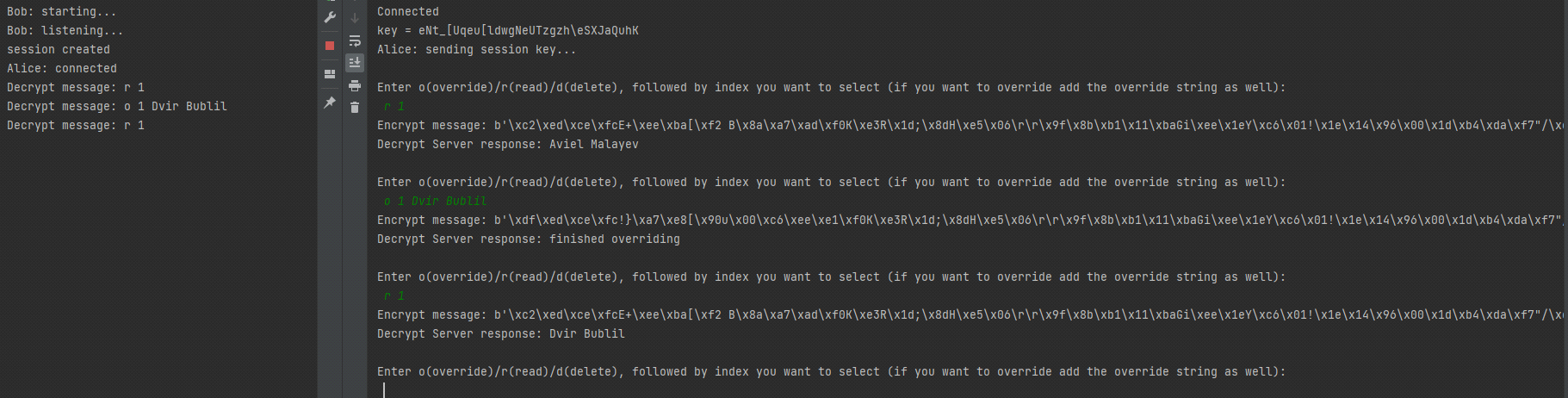
Note: in our system all the messages are sign by ECDSA (including bullet 1-4)

* Bob shares his public key (created by McEliece) to anyone
* Alice generates a key and then she encrypts it with bob’s public key using McEliece Crypto System
* Alice sends the encrypted key to Bob (the session key)
* Bob decrypt’s the message and now both have the same key (the session key) for the symmetric encryption – decryption algorithm (Salsa20)
* Alice takes a message she wants to send to Bob and Encrypt it using Salsa20 algorithm.
* Alice sends to bob the ciphertext and in addition she signs the hashed ciphertext with ECDSA algorithm so that bob could verify it was indeed Alice.
* Bob receives the ciphertext and does the next things:
* Bob decrypt’s the cipher message
* Bob verifies that the sender was Alice using the hashed decrypted cipher text
* Bob does the next things:
* If the message is reading from the DB, Bob sends back the result to Alice
* If the message is override (edit) to the DB than he, does it and notify Alice
* If the message is delete (edit) to the DB than he, does it and notify Alice
* Bob response (1 of 7.3. options) to Alice by send here encrypt response by doing the same action as Alice from 5 until 6
* Alice Repeat Bob's action from 7 until 7.2
* Repeat the process from the 5 again until finishing the connection

**The obtained result:**

**Note: Bob is server and Alice is client**

**Read:**

**Edit:**

**Conclusions:**

* Learning in depth the ciphers and the flow of all the message transportation before starting the work creates safe ground and contributes greatly to the flow of the work itself and the progress in the project stages.
* when asking our lecturer questions regarding our project, we are always getting factual answers that help us to further understand the assignment and the best approach to the solution.
* During work and while learning the algorithms, we realized the importance of encryption in our lives especially as software developers.