For our problem we need to provide to the client a secure way to store their files on the cloud. Because we can’t assure we have a secure channel to transport user’s data, we must cipher every file before send it.

For this, the client’s computer will generate pseudorandom keys and use them to cipher and decipher his files. The user’s file is ciphered using the block cipher AES-256 in mode CBC.

To provide the integrity service we use the HMAC algorithm.

To provide a secure system for our users we must store a copy of their keys on the cloud. We achieve this by using a public-key algorithm to cipher both keys, associated to the uploaded file, the key to decipher the file and the key of the MAC.

Once all the files are ciphered, we can send the data through the net.

To provide the cryptographic services to the user all the operations are in a java script module.