

Figure of the Protocol used in part 2

Program A2 is responsible for creating a Symmetric key, encrypting the OTP key file, and sending it to Bob’s B2 program.

B2 program is responsible for creating Symmetric key and decrypting OTP key.

To generate a Symmetric key, 4 numbers were used:

* P: prime number used as the Modulo
* G: Used as the base to generate the public key only.
* Secret key: Used as the exponent
* Public key of the other person: Used as the base to generate Symmetric key only.

Program A use AES algorithm and Symmetric key to Encrypt the OTP key and send to Bob. Program A also sends Alice’s public key to bob.

Program B use AES algorithm and Symmetric key to Decrypt the OTP key. Program B also sends Bob’s public key to Alice.