README.md

Report for Assignment 2

Usage instructions

1. Make sure you have `python3` installed with the `gmpy2` package. The following commands can achieve that.

   ```
   $ sudo apt install python3 python3-pip
   $ sudo apt install libmpc-dev
   $ pip3 install gmpy2
   ```

   Note that the `gmpy2` library has `libmpc-dev` as requirement.

2. Run the script `trial.py`. It will ask for the message, enter any string in upper case and without any spaces.

   ```
   (venv) sumit@HAL9000:~/Coding/crypto-assignments/A2$ python3 trial.py
   [*] Symmetric key: XATADVUCSMOGBIDTCENRIOBSLRRWCYERQNDGFAKFSFAVDBXRUESOVXMIGSZNMIFCORCGZENCFQWQLRPPVTRLBAYCHYOVSFT
   [*] Enter your message: HELLOWORLD
   --------------------
   [*] Encrypted message: EEELRRITDP
   [*] Encrypted key: BADYPVOIGEZRTQUPLPTOKAVZBPVRSJSIBFBGPSPNFCRYEXEMFCKPSNHNTUZGXWGLATZSFIAHBBKZRHJVMGAPUJHZBAINSXU
   --------------------
   [*] Recovered message: HELLOWORLD
   [*] Recovered key: XATADVUCSMOGBIDTCENRIOBSLRRWCYERQNDGFAKFSFAVDBXRUESOVXMIGSZNMIFCORCGZENCFQWQLRPPVTRLBAYCHYOVSFT
   ```

   It will print out all the information pertaining to the different steps in the pipeline.

Summary of the project

The project has the following python files// modules.

- `genkeys.py` has methods to generate keys for both the symmetric encryption and assymetric encryption.
- `client.py` has methods for encryption and decryption of a message, along with some helper methods. Specifically—
  - The `vignere_encrypt` and `vignere_decrypt` methods are for symmetric encryption and decryption respectively.
  - The `encrypt` and `decrypt` methods carry out the whole encryption and decryption procedure, first symmetric and then assymetric.
  - The `encode` and `decode` methods are helpers for converting string to numeric form and vice-versa.
- `trial.py` is a script that can be used to carry out a sample run of the whole encryption-decryption procedure.

Note—The `rsa_encrypt` method in `client.py` is obsolete can not getting used in the final version of the project, so can be deleted safely. Its functionalites are split and implemented in the rest of the methods discussed above.