**Implementasi Algoritma RSA, ElGamal, Paillier, ECC**

**Laporan Tugas 4**

Diajukan Untuk Memenuhi Tugas 4 IF4020 Kriptografi

Semester I 2021/2022



Disusun oleh

**Reihan Andhika Putra (13519043)**

**Karel Renaldi (13519180)**

**TEKNIK INFORMATIKA**

**INSTITUT TEKNOLOGI BANDUNG**

**BANDUNG**

**2021**

**BAB I**

**Implementasi Program**

**Bahasa Pemrograman : Python**

**Framework : Flask**

1. **RSA.py**

**Text

Description automatically generated**

**Text

Description automatically generated**

1. **Pailler.py**

**Text

Description automatically generated**

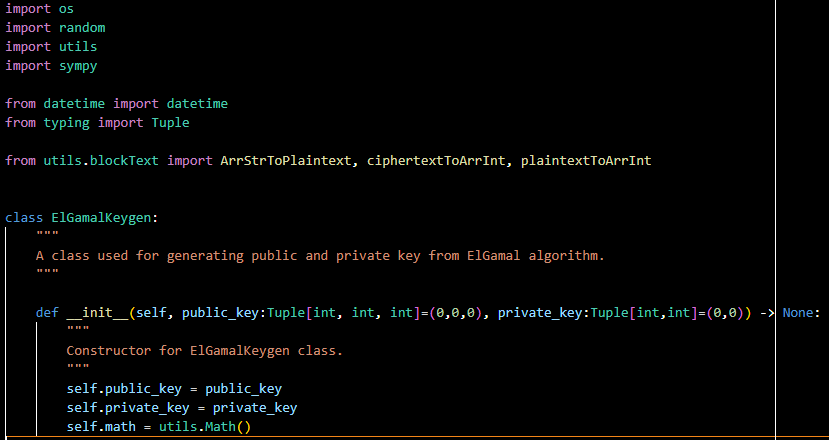
**Text

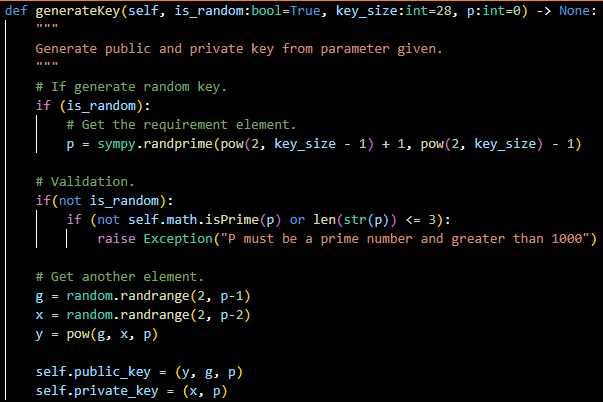
Description automatically generated**

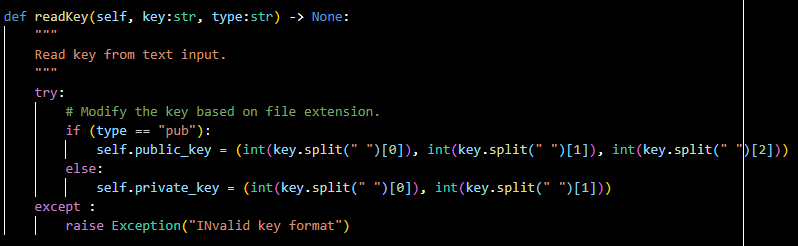
**Text

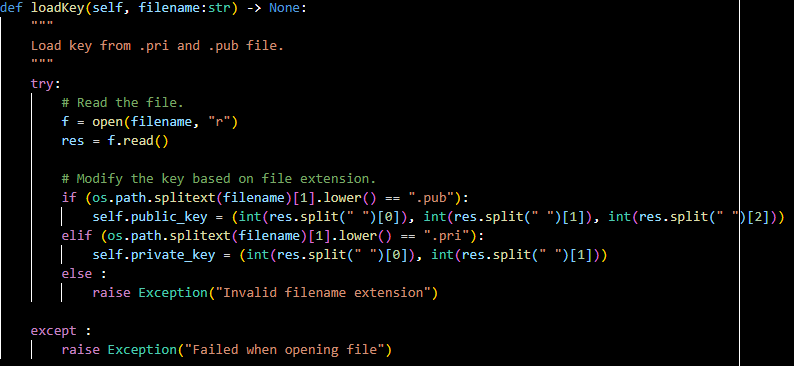
Description automatically generated**

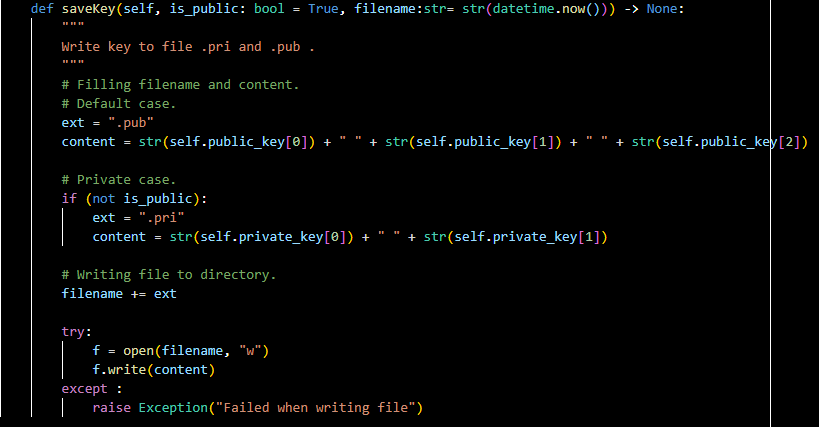
1. **ElGamal.py**

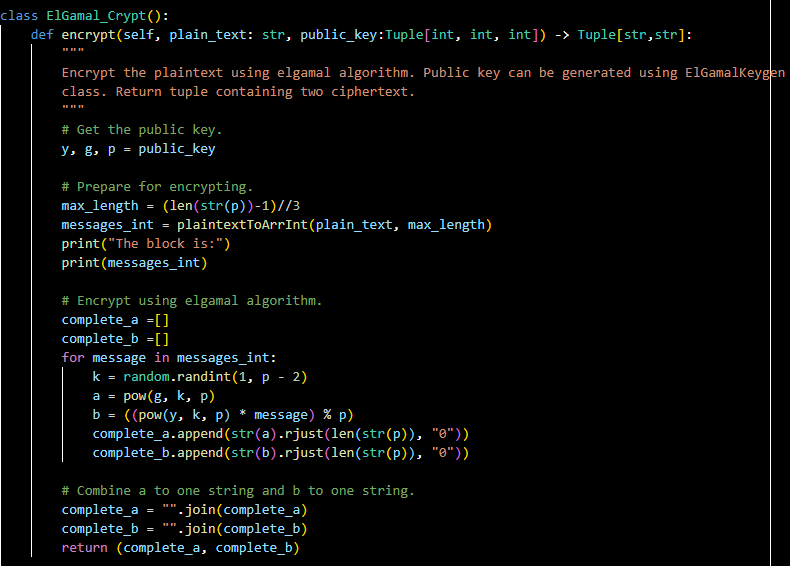


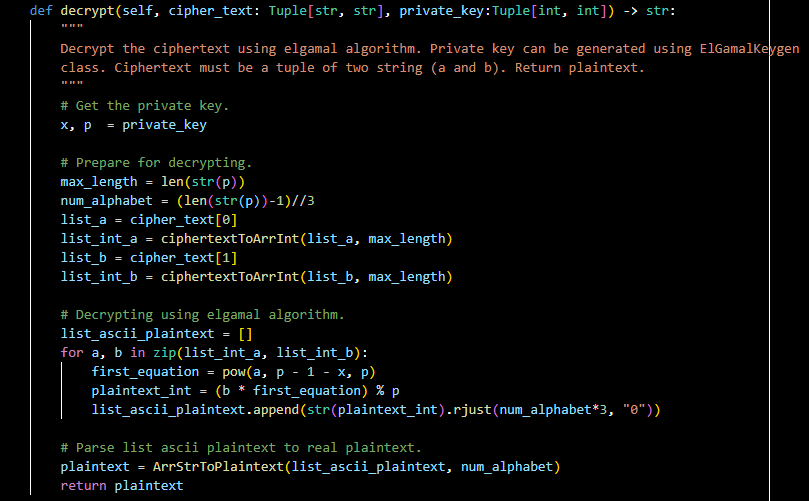




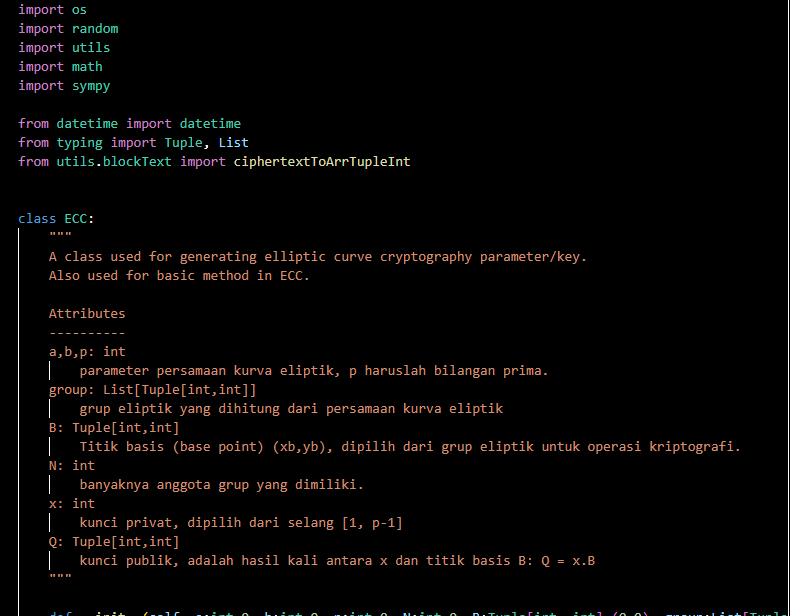


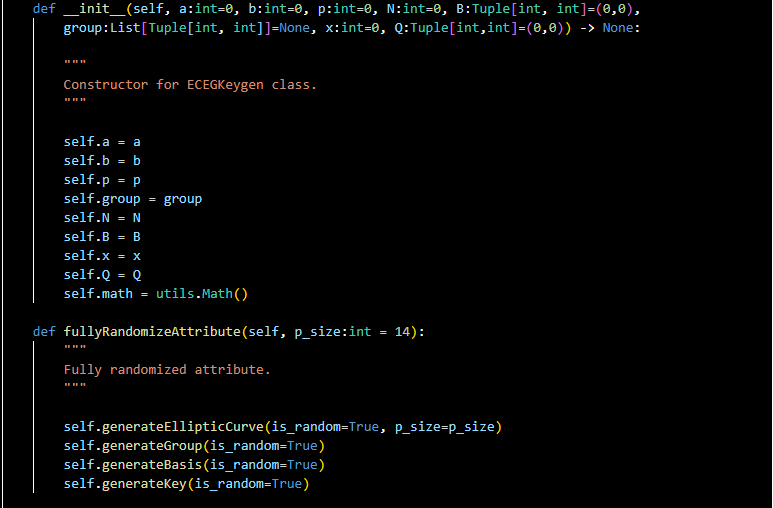


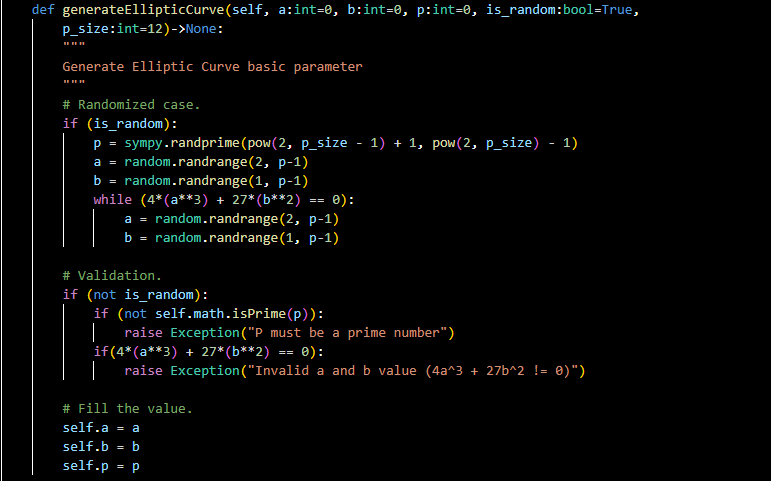


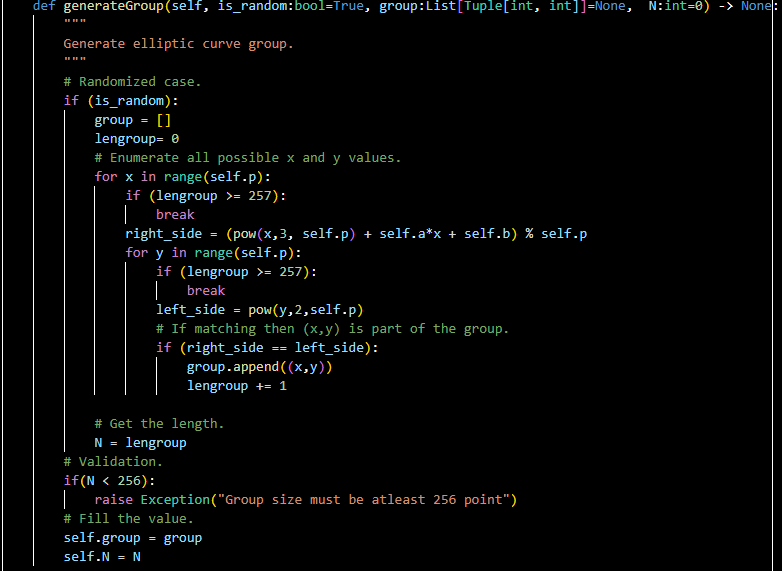


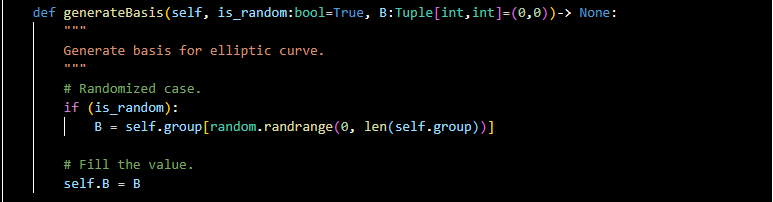
1. **ECEG.py**

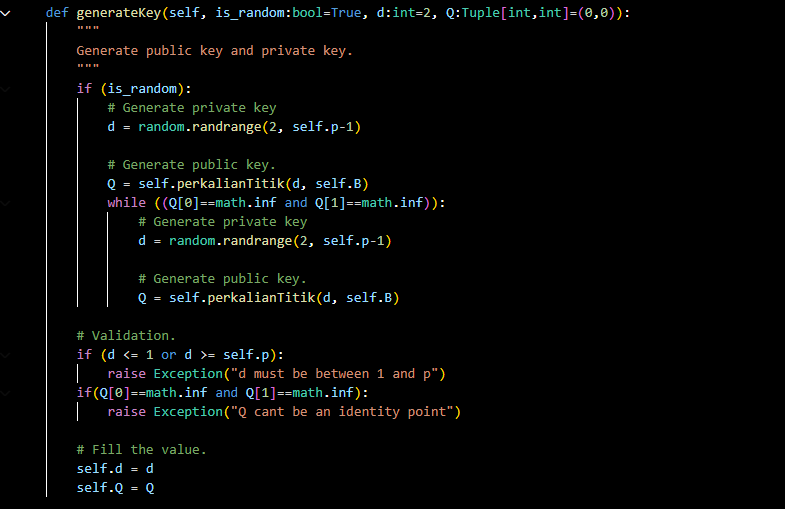


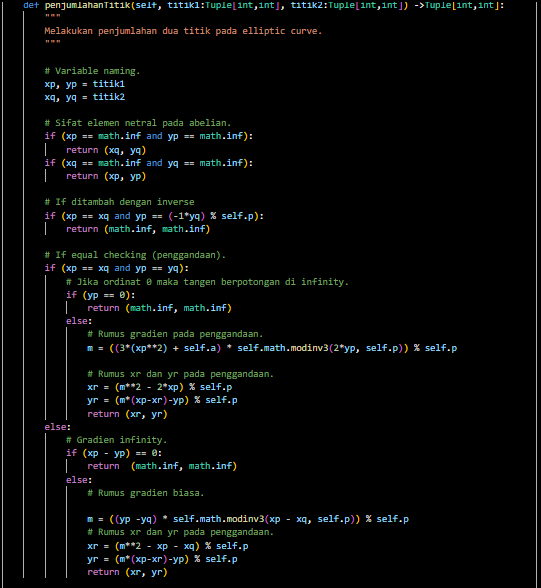


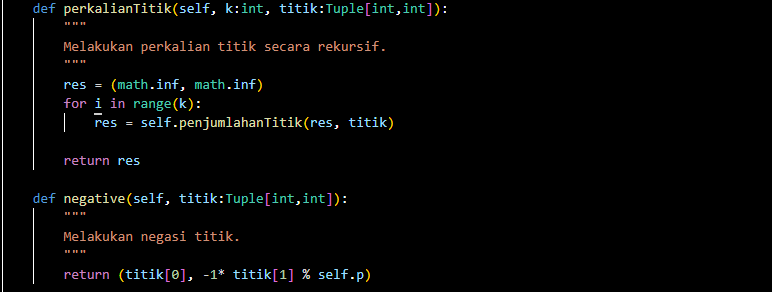


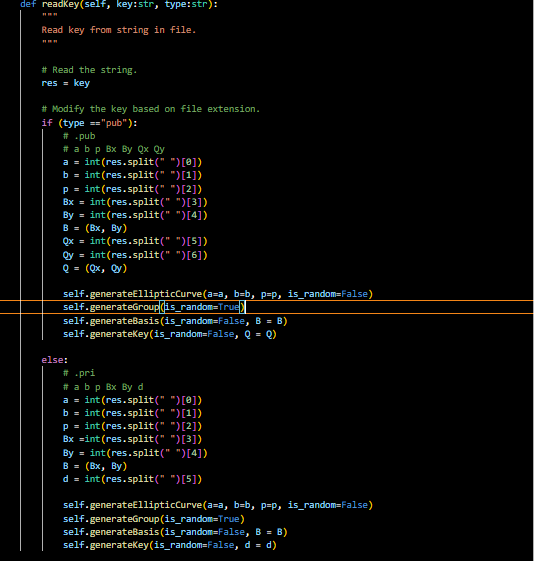


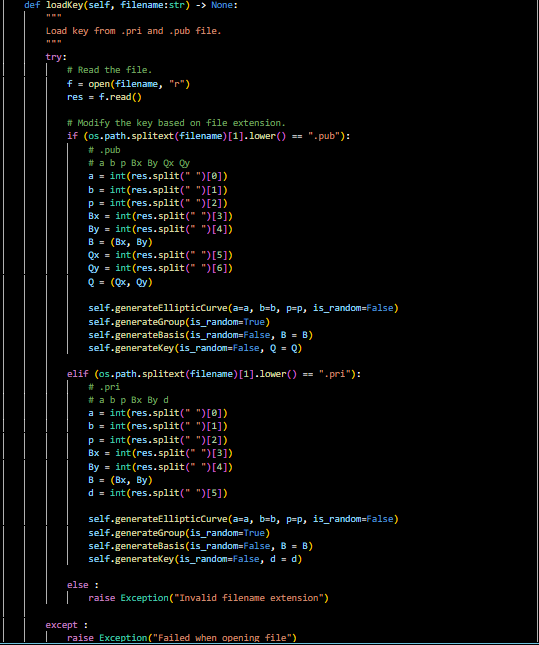


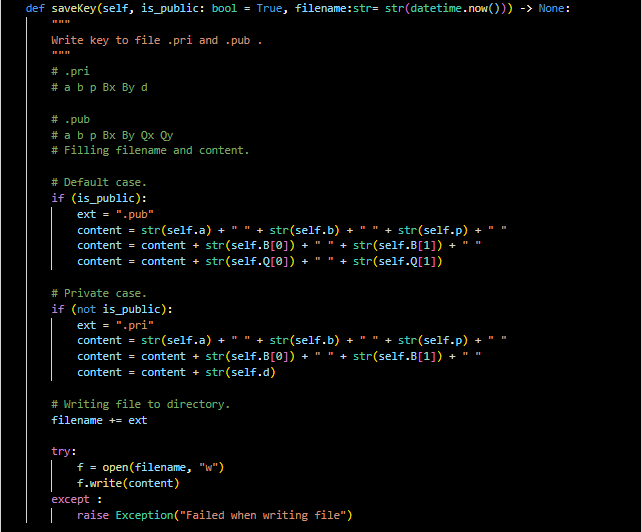


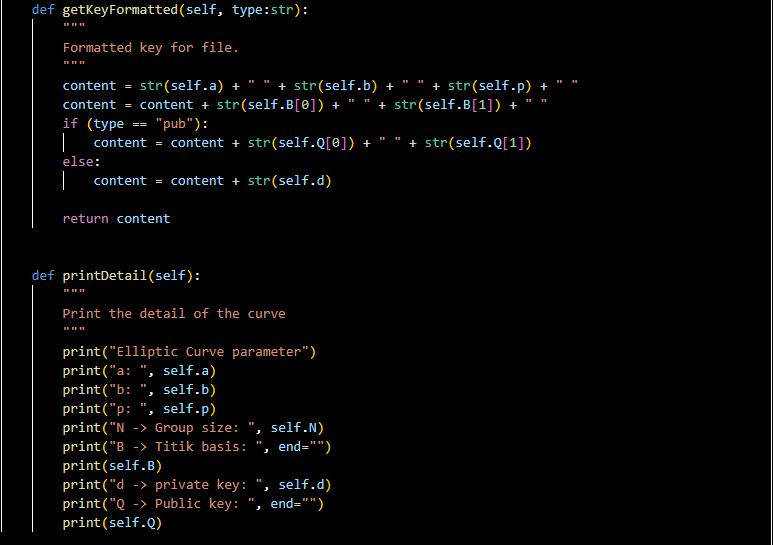


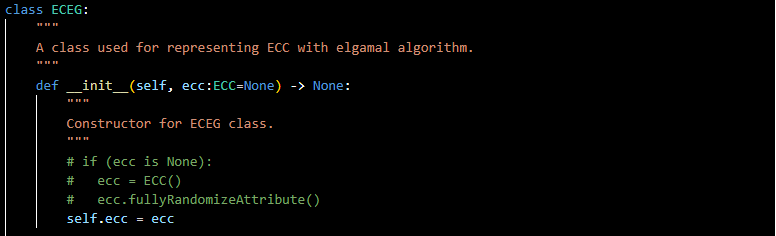


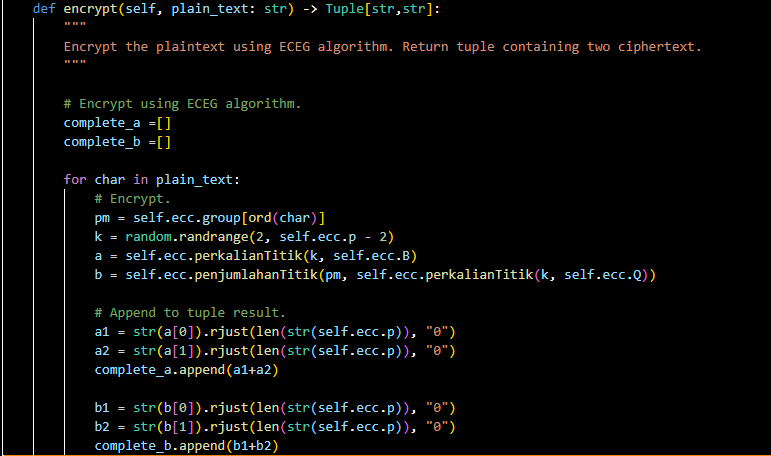


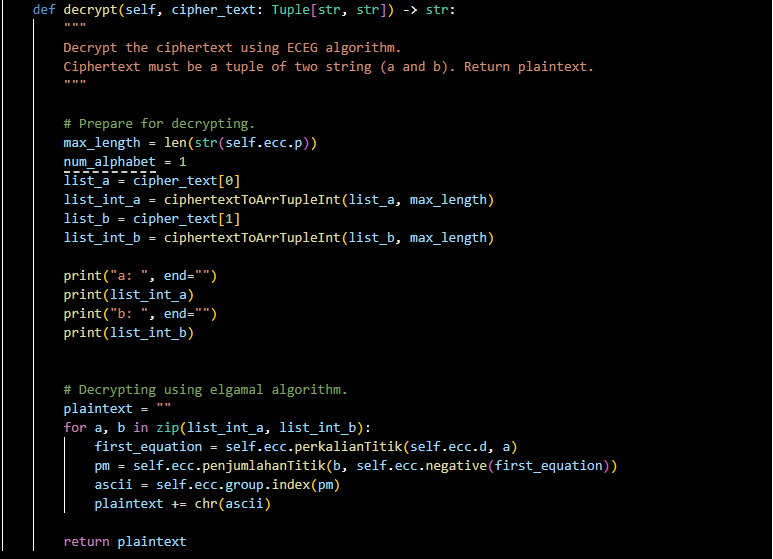




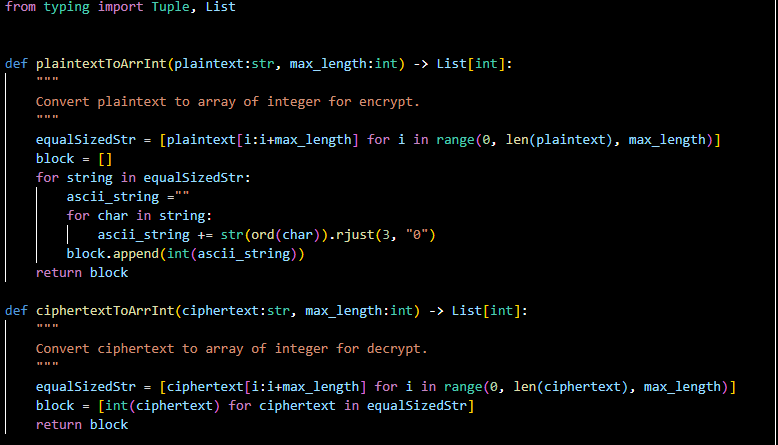


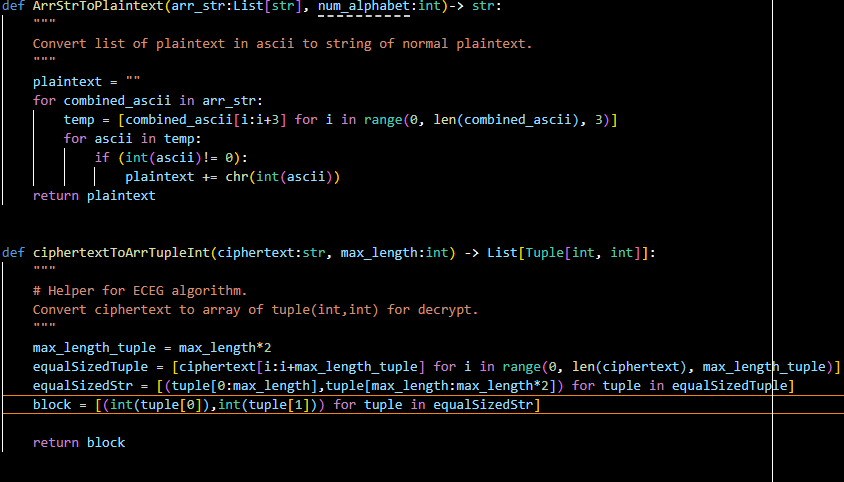




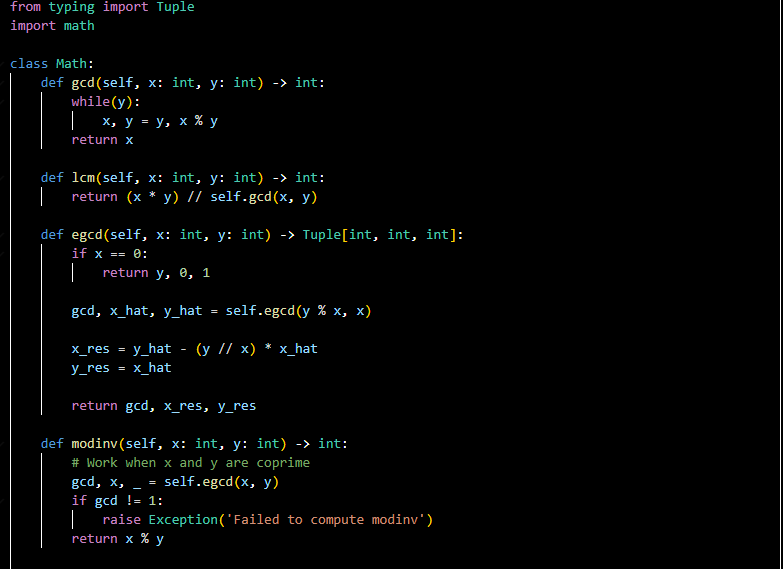


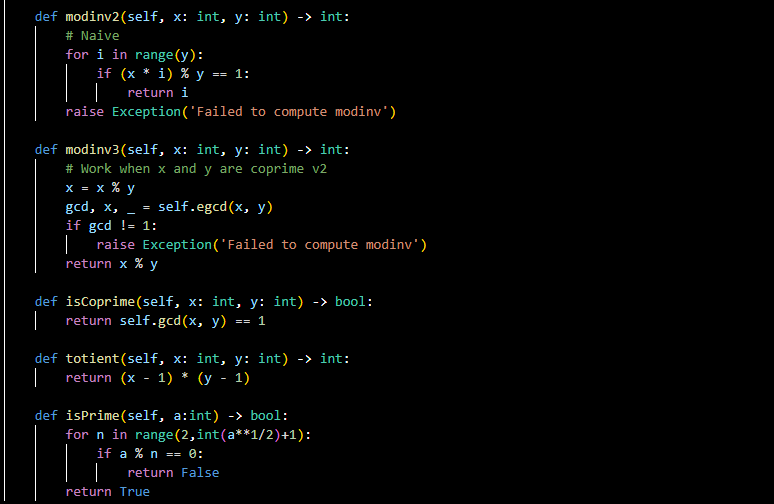
1. **BlockText.py**





1. **Math.py**





**BAB II**

**Tampilan Antarmuka Program**

1. **RSA**

|  |
| --- |
| **Encryption / Decryption** |
|  |

|  |
| --- |
| **Generate Key** |
|  |

1. **Paillier**

|  |
| --- |
| **Encryption / Decryption** |
|  |

|  |
| --- |
| **Generate Key** |
|  |

1. **Elgamal**

|  |
| --- |
| **Encryption/Decryption** |
|  |
|  |

|  |
| --- |
| **Generate Key** |
|  |

1. **ECEG**

|  |
| --- |
| **Encryption/Decryption** |
|  |

|  |
| --- |
| **Generate Key** |
|  |

**BAB III**

**Hasil Percobaan**

*Semua file kunci/text yang disimpan bisa diakses di folder test*

1. **RSA**
   1. **Generate Key**

|  |  |
| --- | --- |
| Ukuran Kunci | 128 |
| Kunci Publik | rsa\_key.pub |
| Kunci Privat | rsa\_key.pri |
| Hasil | |
|  | |

* 1. **Enkripsi**

|  |  |
| --- | --- |
| Kunci Publik | rsa\_key.pub |
| Ciphertext Hasil | rsa\_cipher.txt |
| Plaintext | Di suatu siang yang terik, seekor burung gagak merasa sangat kehausan. |
| Hasil | |
|  | |

* 1. **Dekripsi**

|  |  |
| --- | --- |
| Kunci Privat | rsa\_key.pri |
| Ciphertext | rsa\_cipher.txt |
| Plaintext Hasil | Di suatu siang yang terik, seekor burung gagak merasa sangat kehausan |
| Hasil | |
|  | |

1. **Pallier**
   1. **Generate Key**

|  |  |
| --- | --- |
| Ukuran Kunci | 128 |
| Kunci Publik | pallier\_key.pub |
| Kunci Privat | pallier\_key.pri |
| Hasil | |
|  | |

* 1. **Enkripsi**

|  |  |
| --- | --- |
| Kunci Publik | pallier\_key.pub |
| Plaintext | Di suatu siang yang terik, seekor burung gagak merasa sangat kehausan. |
| Ciphertext Hasil | pallier\_cipher.txt |
| Hasil | |
|  | |

* 1. **Dekripsi**

|  |  |
| --- | --- |
| Kunci Privat | pallier\_key.pri |
| Ciphertext | pallier\_cipher.txt |
| Plaintext Hasil | Di suatu siang yang terik, seekor burung gagak merasa sangat kehausan. |
| Hasil | |
|  | |

1. **Elgamal**
   1. **Generate Key**

|  |  |
| --- | --- |
| Ukuran Kunci | 128 |
| Kunci Publik | elgamal\_key.pub |
| Kunci Privat | elgamal\_key.pri |
| Hasil | |
|  | |

* 1. **Enkripsi**

|  |  |
| --- | --- |
| Kunci Publik | Elgamal\_key.pub |
| Plaintext | Hidup lebih dari harus sekedar tetap hidup. Masalahnya, bagaimana membuat hidup itu bermakna, memancarkan cahaya gemilang ke masa depan, sekalipun harus mengorbankan hidup itu sendiri. Bila ini sudah tercapai, maka tidak ada bedanya dengan berapa lama hidup itu. (Mushashi) |
| Ciphertext | ciphertext\_elgamal\_1.txt, ciphertext\_elgamal\_2.txt |
| Hasil | |
|  | |

* 1. **Dekripsi**

|  |  |
| --- | --- |
| Kunci Privat | elgamal\_key.pri |
| Ciphertext | ciphertext\_elgamal\_1.txt, ciphertext\_elgamal\_2.txt |
| Plaintext | plaintext\_elgamal.txt |
| Hasil | |
|  | |

1. **ECEG**
   1. **Generate Key**

|  |  |
| --- | --- |
| Ukuran Kunci | 16 |
| Kunci Publik | eceg\_key.pub |
| Kunci Privat | eceg\_key.pri |
| Hasil | |
|  | |

* 1. **Enkripsi**

|  |  |
| --- | --- |
| Kunci Publik |  |
| Plaintext | Hidup lebih dari harus sekedar tetap hidup. Masalahnya, bagaimana membuat hidup itu bermakna, memancarkan cahaya gemilang ke masa depan, sekalipun harus mengorbankan hidup itu sendiri. Bila ini sudah tercapai, maka tidak ada bedanya dengan berapa lama hidup itu. (Mushashi) |
| Ciphertext | ciphertext\_eceg\_1.txt, ciphertext\_eceg \_2.txt |
| Hasil | |
|  | |

* 1. **Dekripsi**

|  |  |
| --- | --- |
| Kunci Privat | elgamal\_key.pri |
| Ciphertext | ciphertext\_eceg\_1.txt, ciphertext\_eceg \_2.txt |
| Plaintext | plaintext\_eceg.txt |
| Hasil | |
|  | |

**BAB IV**

**Lampiran**

1. **Pranala github yang berisi kode program**

https://github.com/AndhikaRei/Modern-Cryptography