Laporan Tugas Kecil 3

Implementasi Algoritma RSA, Elgamal, dan Diffie-Hellman

IF4020 Kriptografi

Dibuat oleh:

Farras Mohammad Hibban Faddila 13518017

M. Fauzan Rafi Sidiq Widjonarto 13518147

PROGRAM STUDI TEKNIK INFORMATIKA

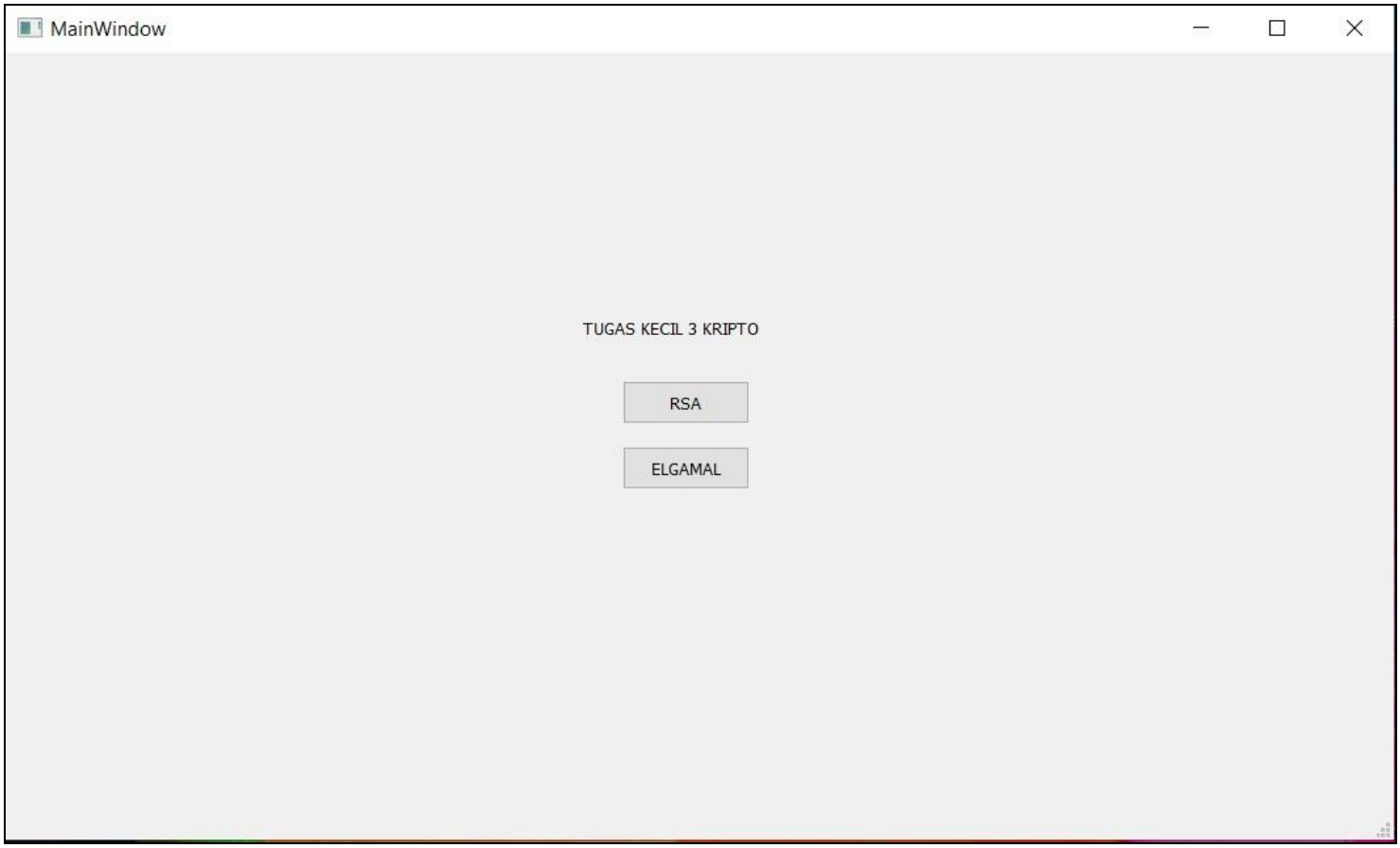
SEKOLAH TEKNIK ELEKTRO DAN INFORMATIKA

INSTITUT TEKNOLOGI BANDUNG

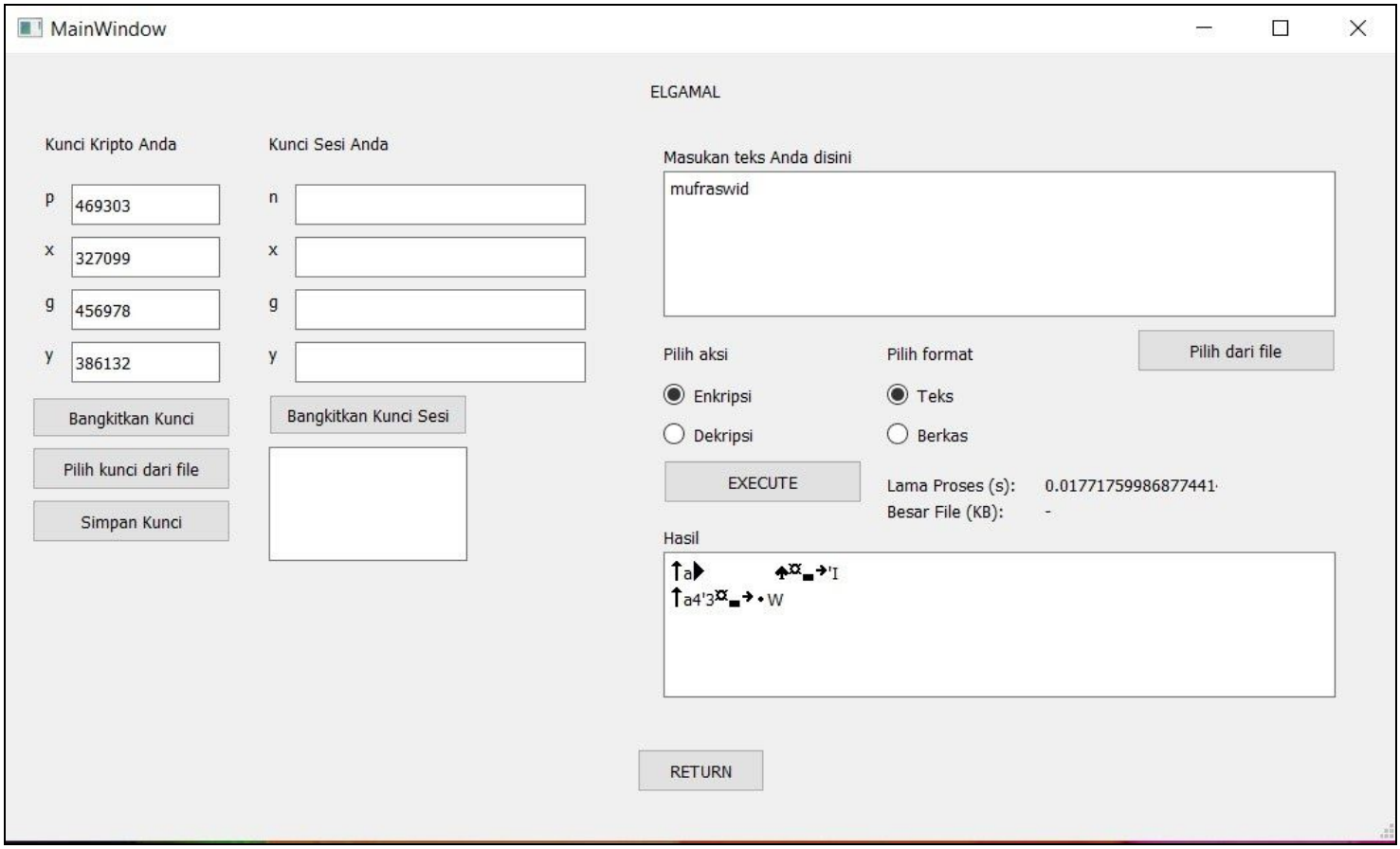
2020

A. Tampilan Antar Muka Program

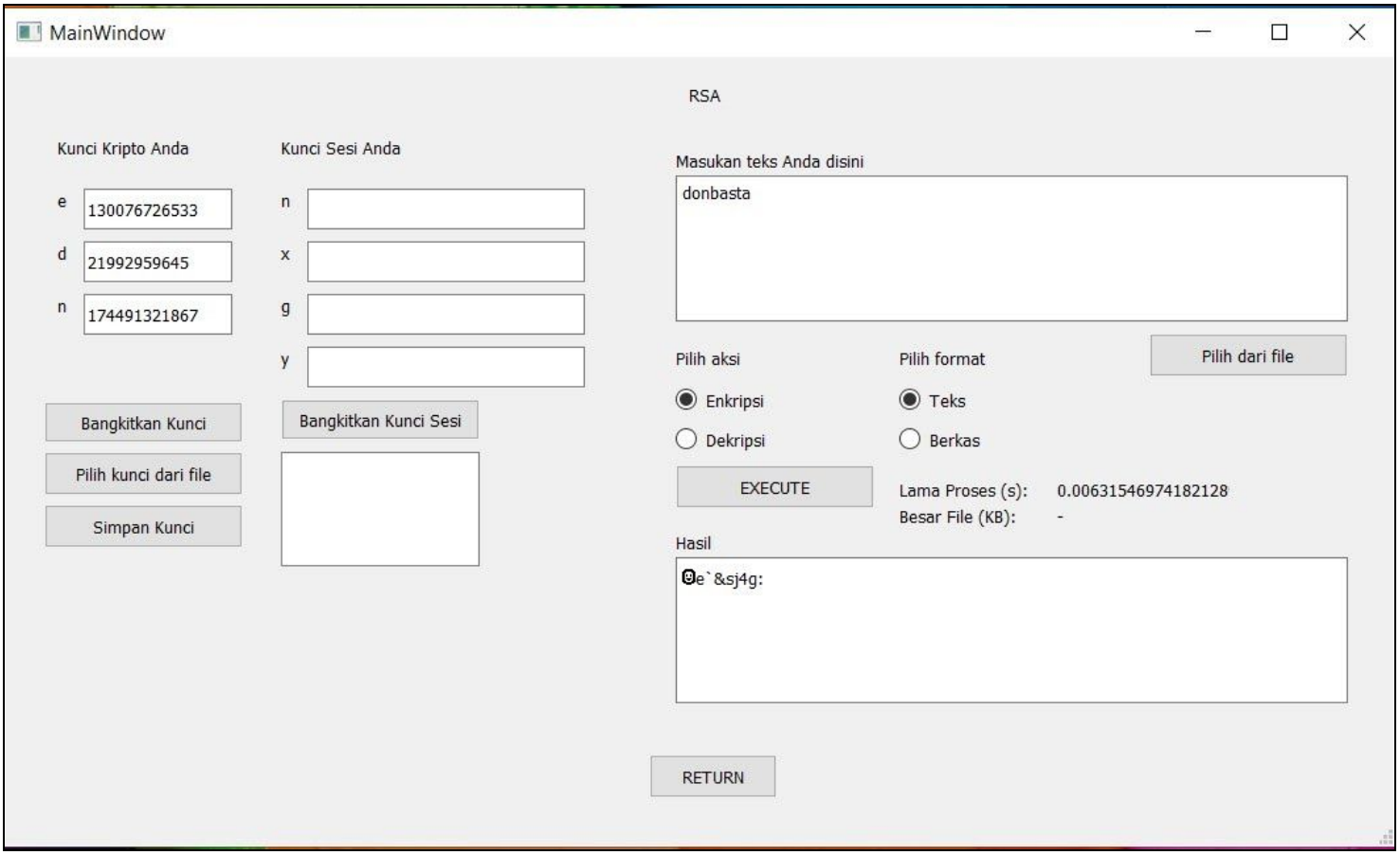
- **Tampilan Menu Utama**



- **Tampilan Menu Elgamal**

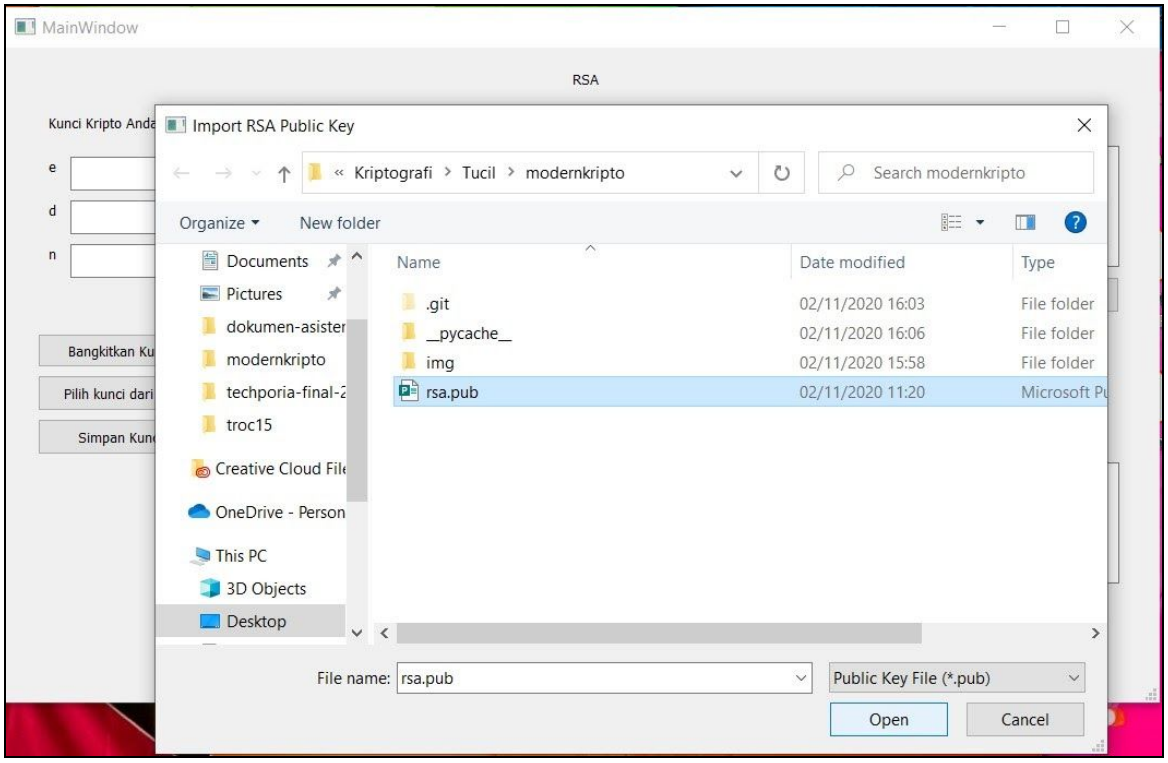


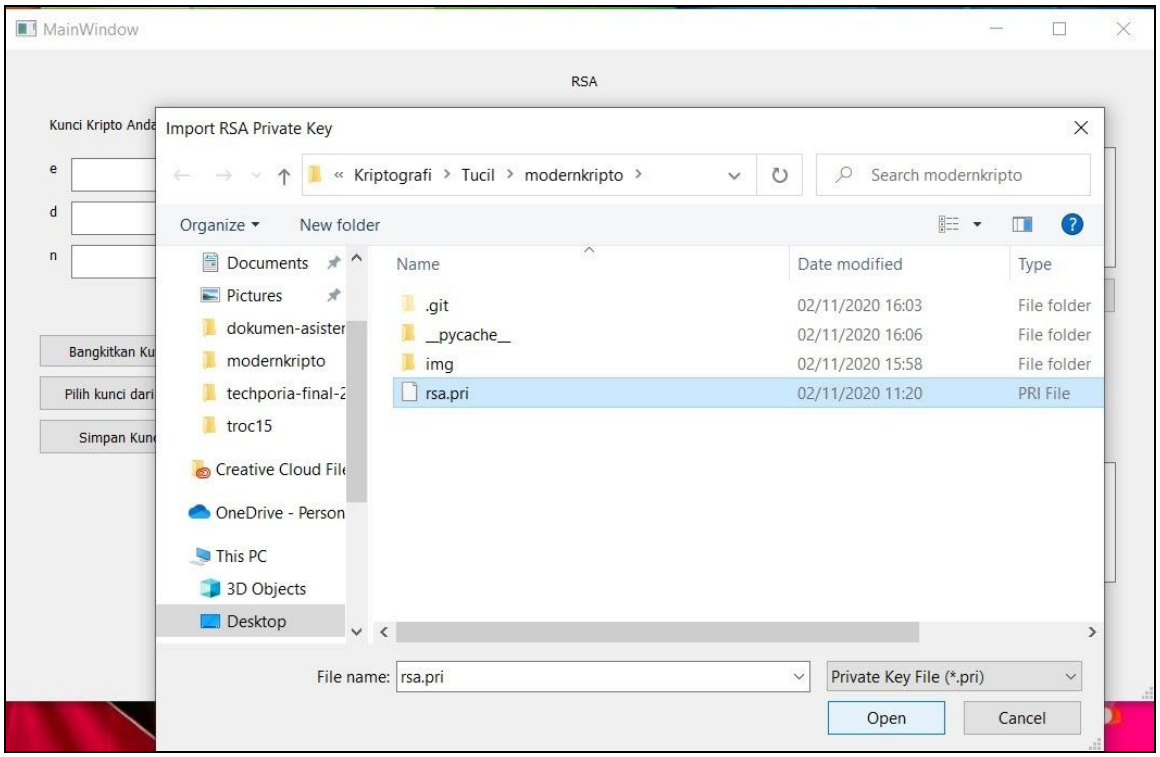
- **Tampilan Menu RSA**



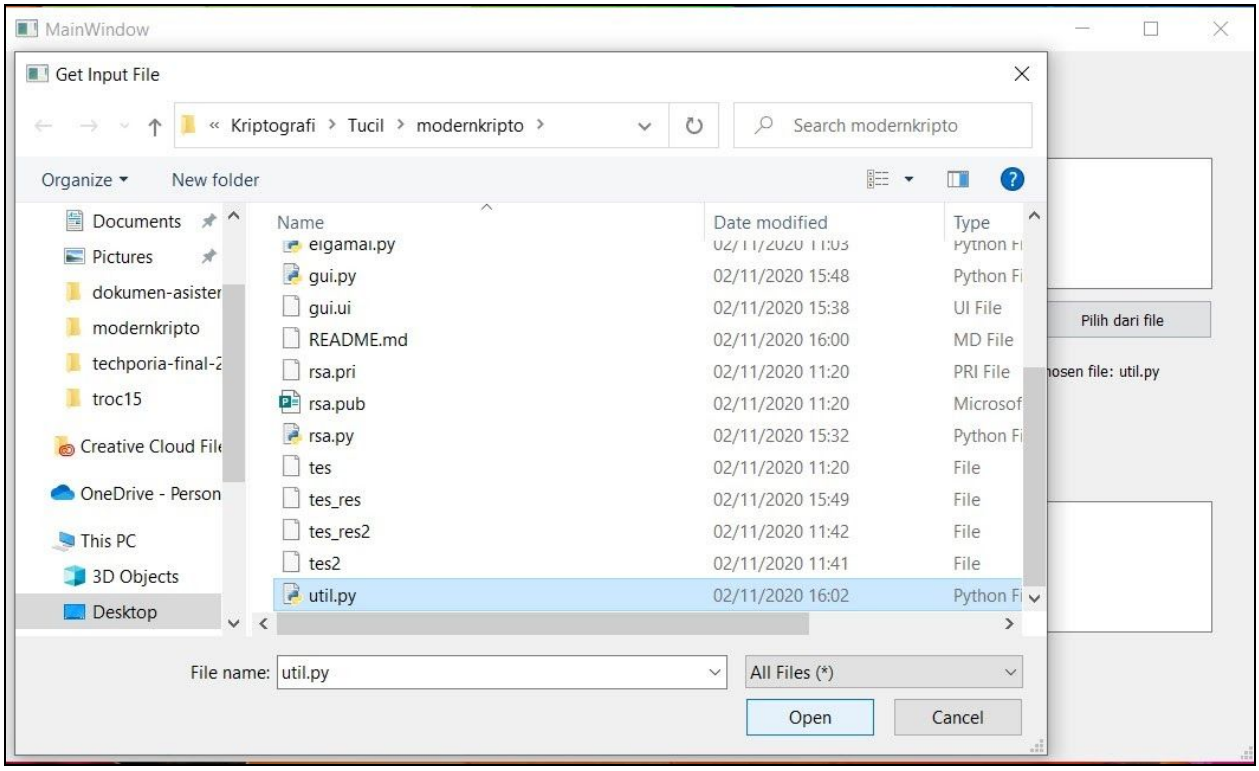
(Catatan: Pembangkitan kunci sesi Diffie Hellman terdapat pada kedua menu tersebut)

- **Import Key from External File**

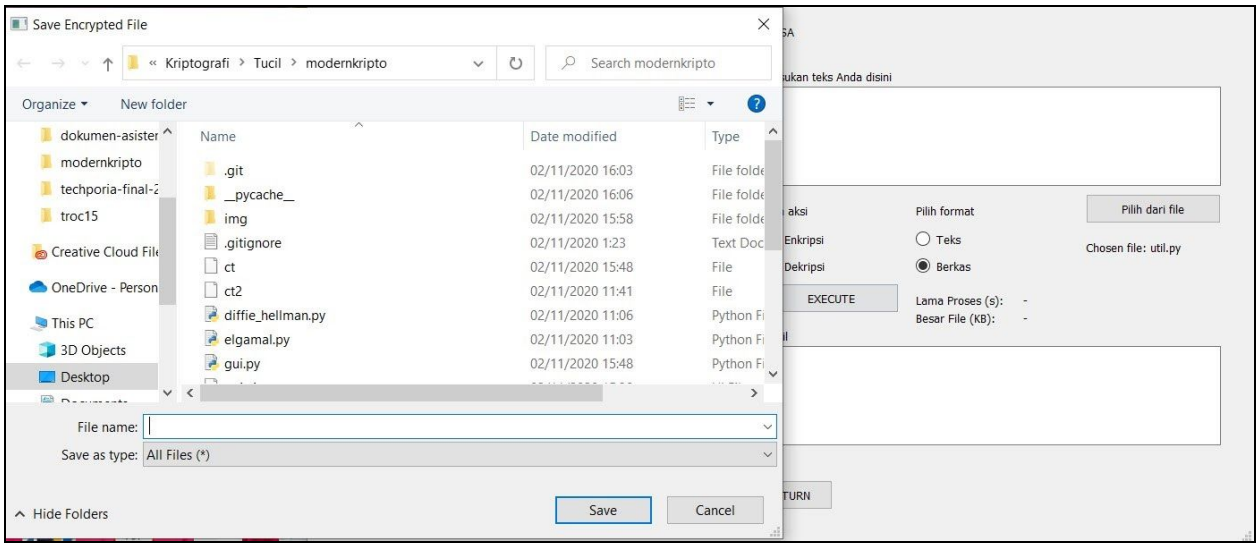




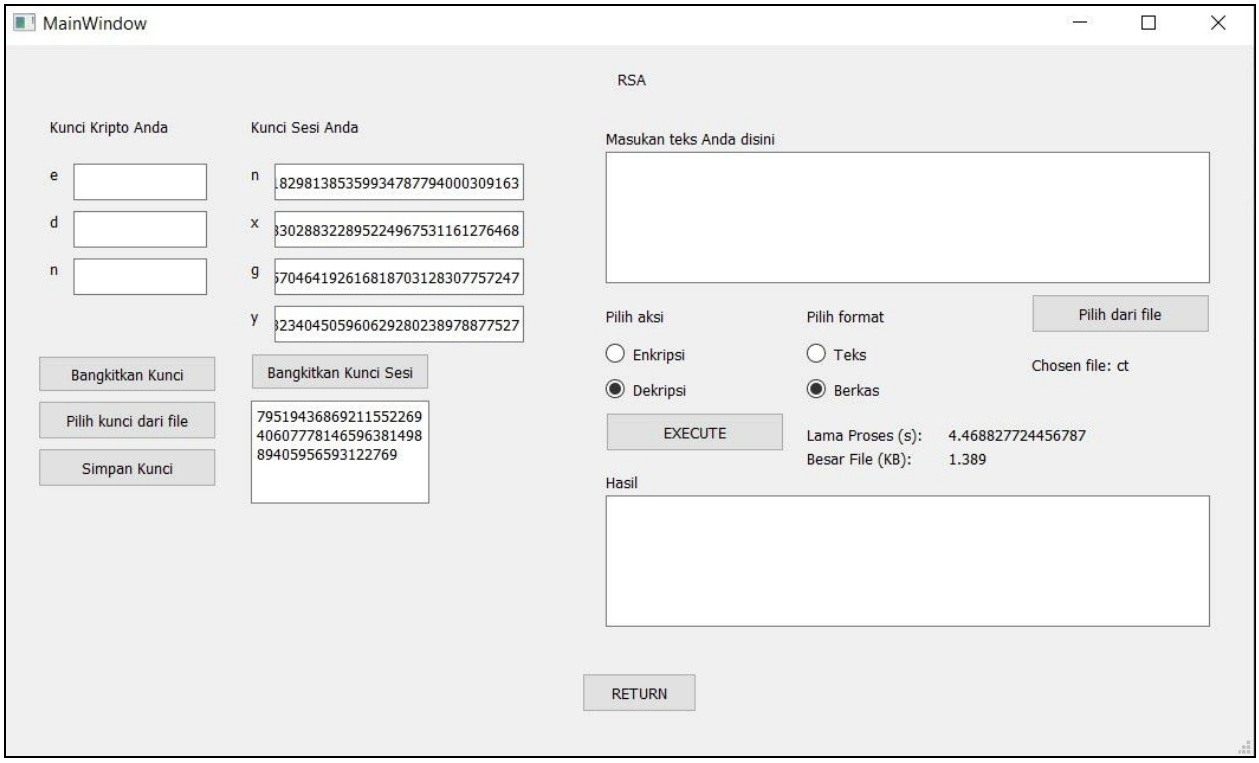
- **Get Plaintext from External File**



- **Save Ciphertext to External File**



- **Pembangkitan Kunci Sesi**



C. Contoh Pengujian

1. Pengujian Algoritma RSA

    a. Kasus Uji 1 (Teks)

Plaintext : Hehehe

Ciphertext : YXUV%Es7sf62AUW0Ids"01I 4j

n : 384876874936566887243214420310243103270575901088551162766877588864349561074 1

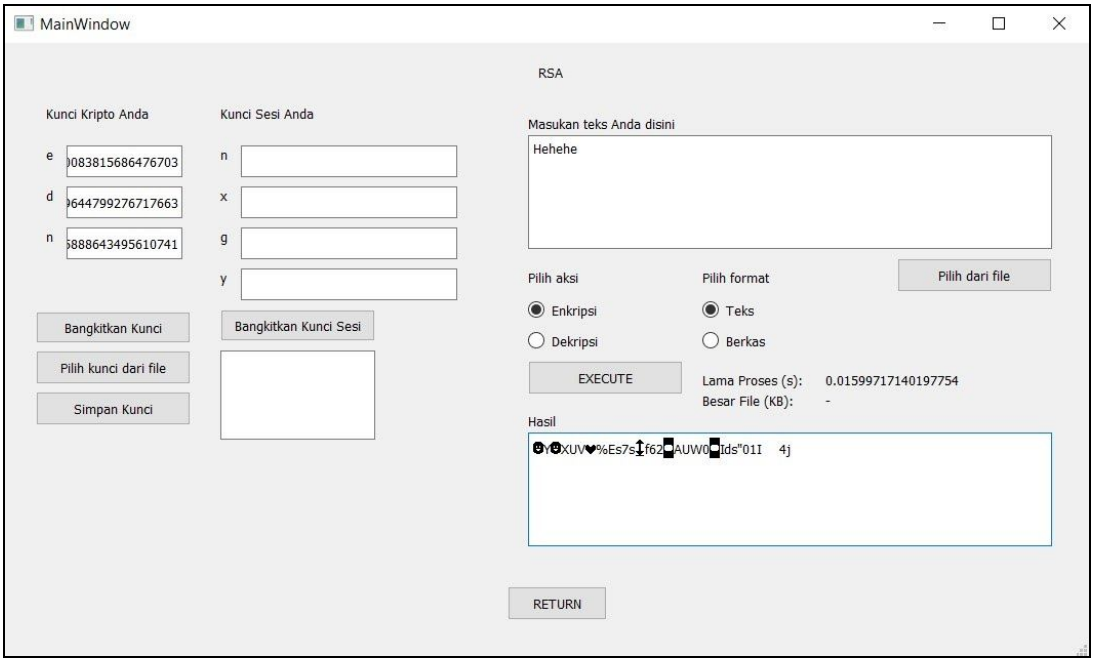
d : 27546332132878874515038115042698234998699885575921680552920296447992767176 63

e : 17519368951437356517780158133046811056012719747247910145386200838156864767 03

Nilai p dan q yang digenerate secara random: (Rahasia)

p : 67336560354985573680467241513391525153

q : 57157192601993479718128319601872125397



    b. Kasus Uji 2 (Berkas)

Plaintext : pt (nama berkas)

Ciphertext : ct (nama berkas)
Isi berkas pt: haha hihi huhu hehe hoho besok tubes

Isi berkas ct: 3273 7969 ab0f f398 7018 6ab0 ff99 0310 58ab 0ff1 1007 797a b0ff 6842 7832 ab1f f808 1347 6ab1 ff90 4630 22ab 0ff5 1302 966a b0ff 9668 008a b0ff 3410 5841 ab0f f937 4741 5ab0

n :
4506912902513682148451671163655217172597958421586045487795207035867357557140937563308653576713585417 3107

d
:189114773051990898819111789967653253264713047348964035556140547388901143688083308053939592528211895 154203

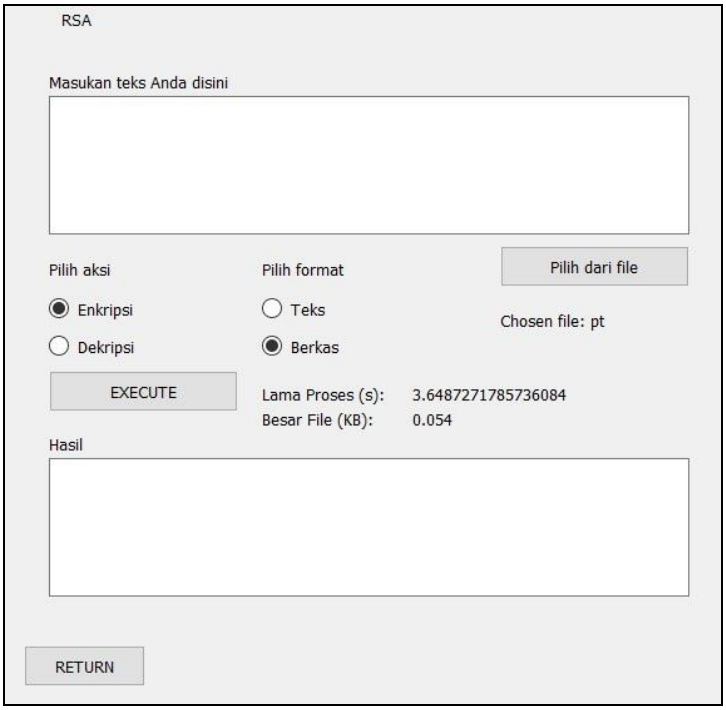
e :
274233606793070319711173859452162612357731965655685173497471145993066931367196325799077831624299905285137

Nilai p dan q yang digenerate secara random: (Rahasia)

p : 142309224532682122952295395484562215278183830808261 17

q : 192702621838889306792260130692786249338023330700760 61

Waktu: 3.68s
Ukuran file eksternal: 0.054 KB



2. Pengujian Algoritma Elgamal
    a. Kasus Uji 1 (Teks)

Plaintext: aku sangat suka tubes

Ciphertext:(*()VZ(tVA(Z(J((@j(3□:((J(t!

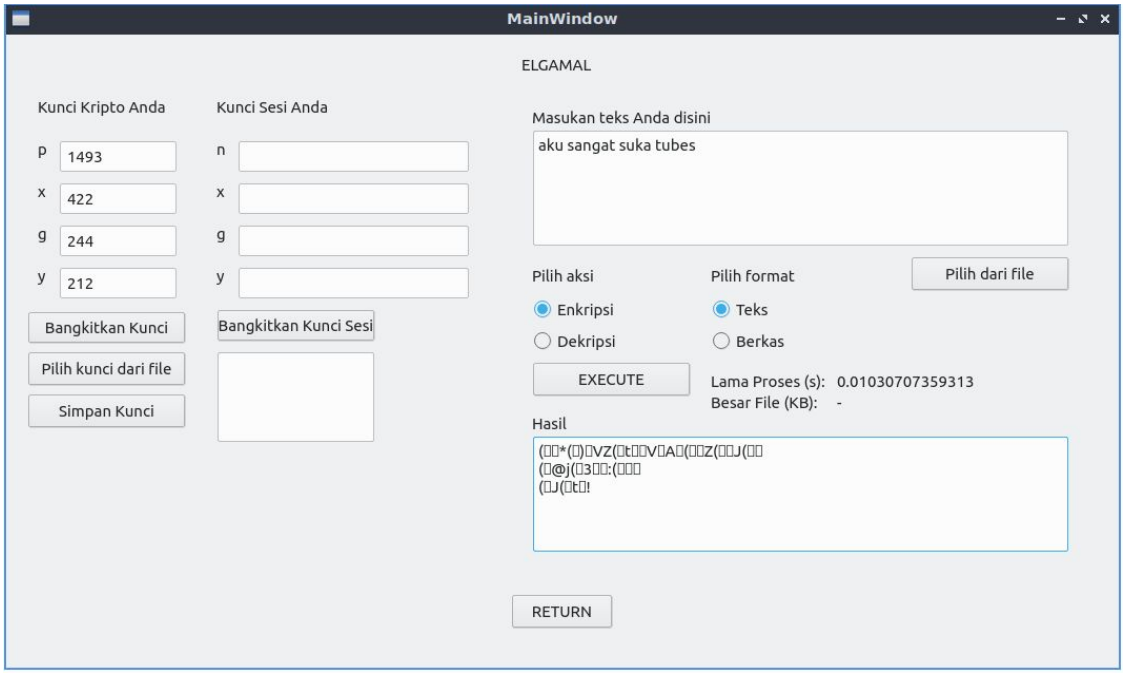
P = 1493

G = 244

Y = 212

Nilai X (Rahasia):
X = 422

Waktu: 0.0103 sekon



    b. Kasus Uji 2 (Berkas)

Plaintext: hihi.txt
Isi: aku sangat suka tubes kuriputogurafi

Ciphertext:
"

```
�`��"
�e���"
��I���  �!� ��"
�af*��  ��#v��"
�`��"
�CFj��  ��%e9��"
�gZ��  ��9$��"
�dX��"
�v��"
�i%j��  ��x���"
�a��"
�I2��
```

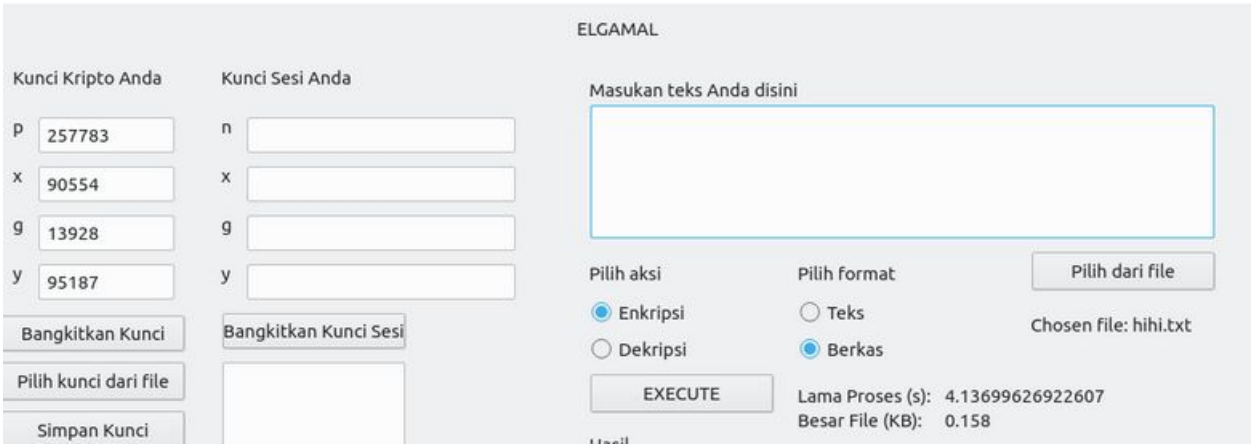

P = 257783

G = 13928

Y = 95187

Nilai X (Rahasia):
X = 90554

Waktu: 4.136 sekon
Besar file ciphertext : 0.158 KB



3. Pengujian Algoritma Diffie-Hellman untuk Pembangkitan Kunci Sesi

   Nilai g dan n adalah prima besar dibangkitkan secara random dengan library PyCryptodome, dan x, y juga dibangkitkan secara random sebagai berikut:

   n = 348771428620185844368239975903817870666765789647 9
   g = 476891397066346964511830008614700754886354 7

x = 484348003034230608719159349442130504 71
y = 100699051630208396184019302779444991 68

Key: 3108289229465528903152639404311030864133984309552