

Laporan Tugas Kecil 3
Implementasi Algoritma RSA, Elgamal, dan Diffie-Hellman
IF4020 Kriptografi



Dibuat oleh:

Farras Mohammad Hibban Faddila 13518017

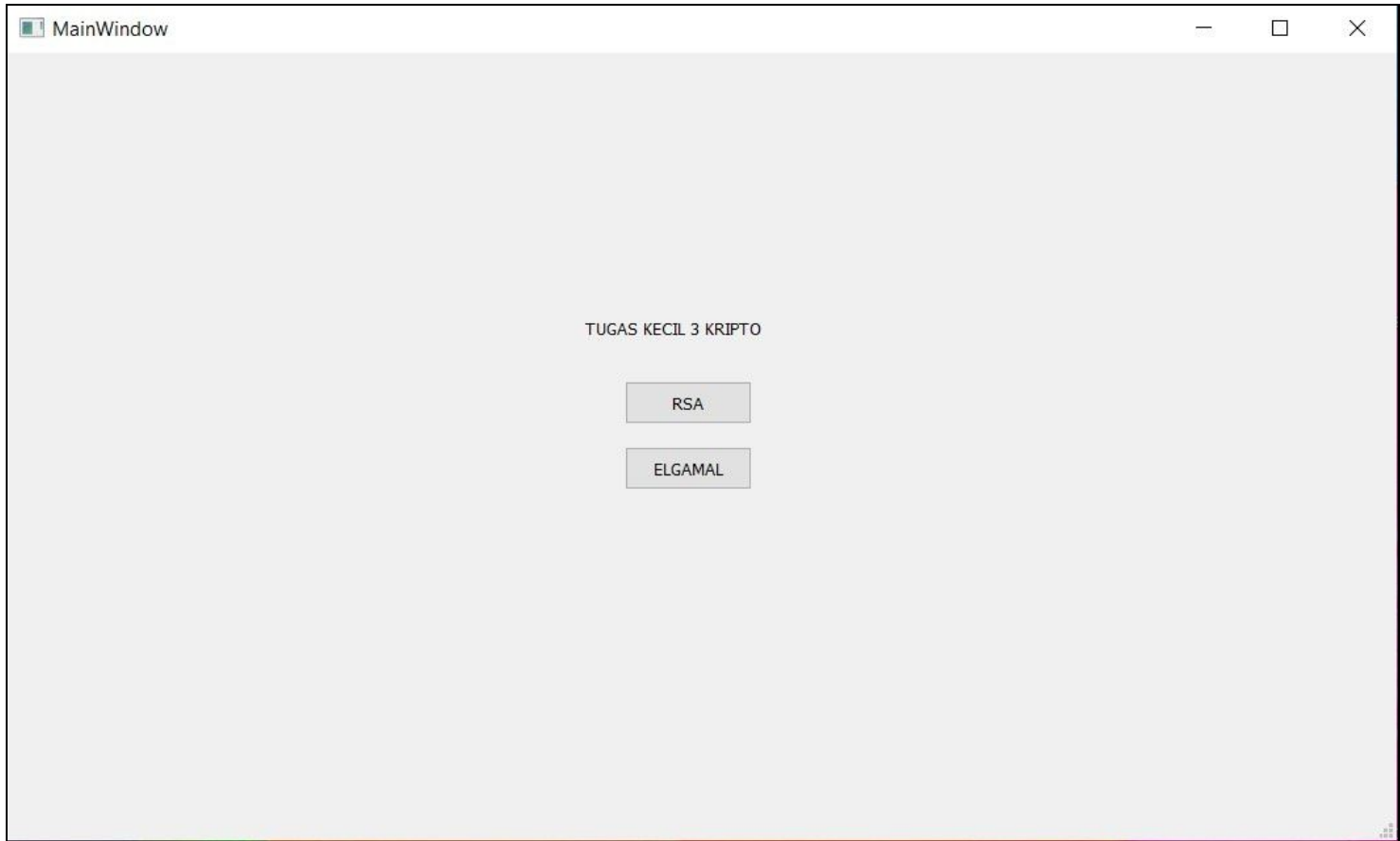
M. Fauzan Rafi Sidiq Widjonarto 13518147

PROGRAM STUDI TEKNIK INFORMATIKA
SEKOLAH TEKNIK ELEKTRO DAN INFORMATIKA
INSTITUT TEKNOLOGI BANDUNG

2020

A. Tampilan Antar Muka Program

- Tampilan Menu Utama



- **Tampilan Menu Elgamal**

MainWindow

ELGAMAL

Kunci Kripto Anda

P469303

x327099

g456978

Y386132

Bangkitkan Kunci

Pilih kunci dari file

Simpan Kunci

Kunci Sesi Anda

n

x

g

y

Bangkitkan Kunci Sesi

Masukan teks Anda disini

mufRASwid

Pilih aksi

☒ Enkripsi

☐ Dekripsi

Pilih format

☒ Teks

☐ Berkas

Pilih dari file

EXECUTE

Lama Proses (s): 0.01771759986877441

Besar File (KB): -

Hasil

↑a▶↕⌘→'I
↑a4'3⌘→•W

RETURN

- **Tampilan Menu RSA**

MainWindow

RSA

Kunci Kripto Anda

e 130076726533

d 21992959645

n 174491321867

Bangkitkan Kunci

Pilih kunci dari file

Simpan Kunci

Kunci Sesi Anda

n

x

g

y

Bangkitkan Kunci Sesi

Masukan teks Anda disini

donbasta

Pilih aksi

☒ Enkripsi

☐ Dekripsi

Pilih format

☒ Teks

☐ Berkas

Pilih dari file

EXECUTE

Lama Proses (s): 0.00631546974182128

Besar File (KB): -

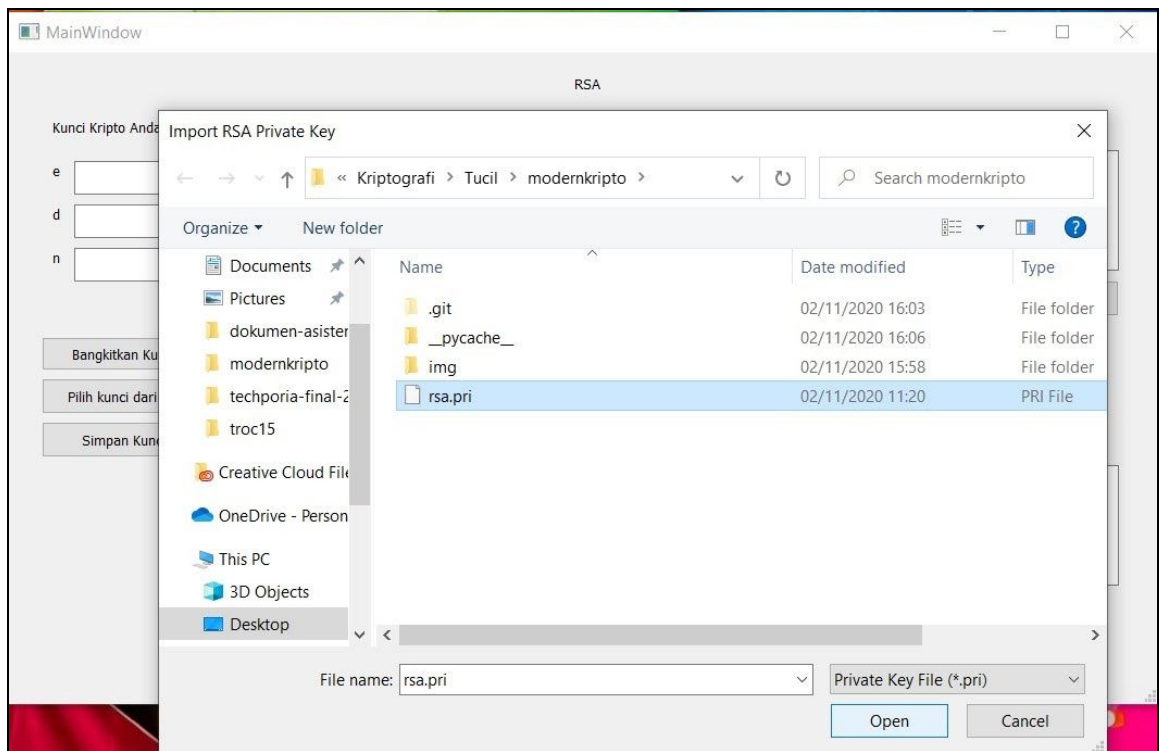
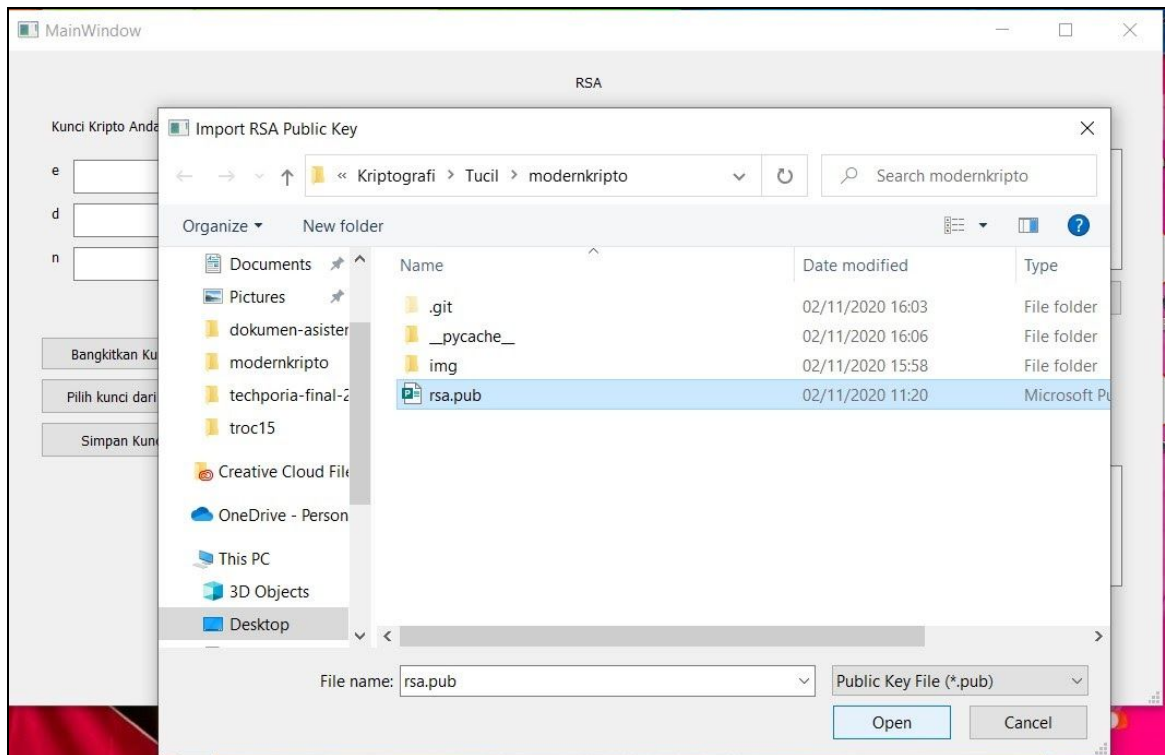
Hasil

0e`&sj4g:

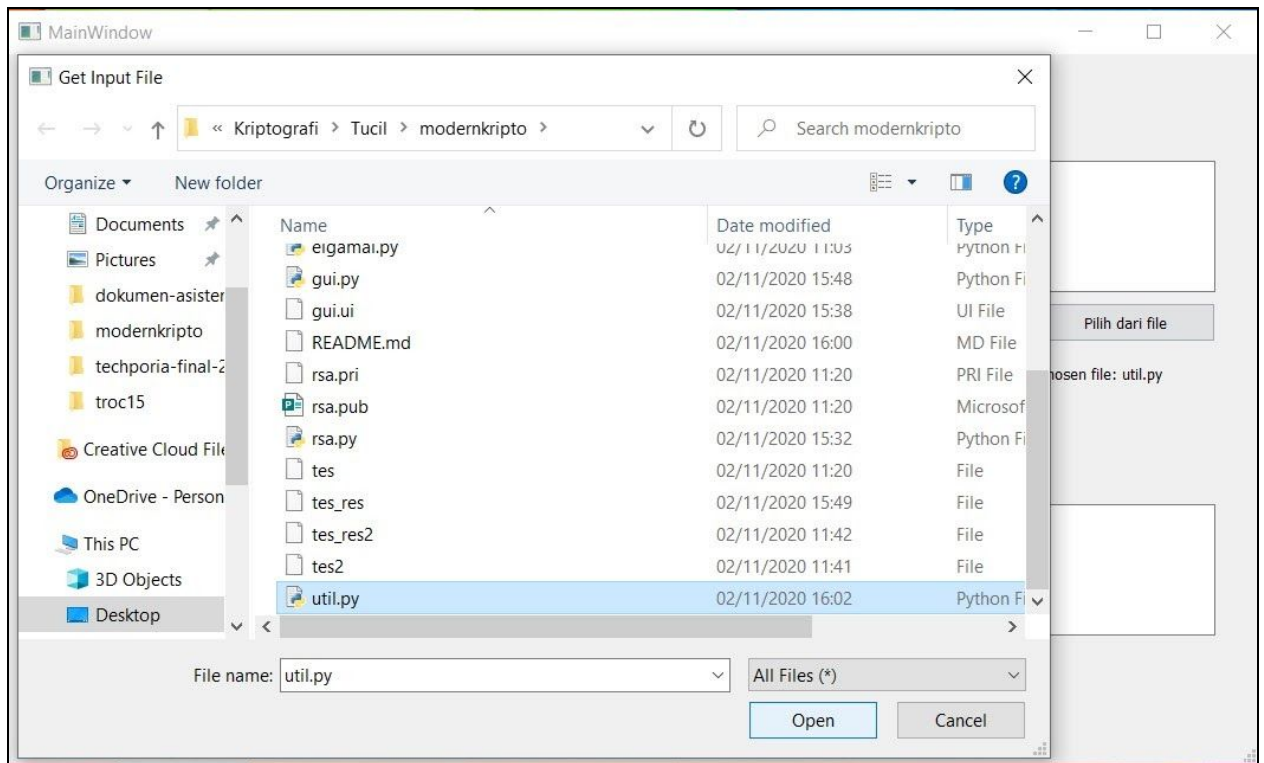
RETURN

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

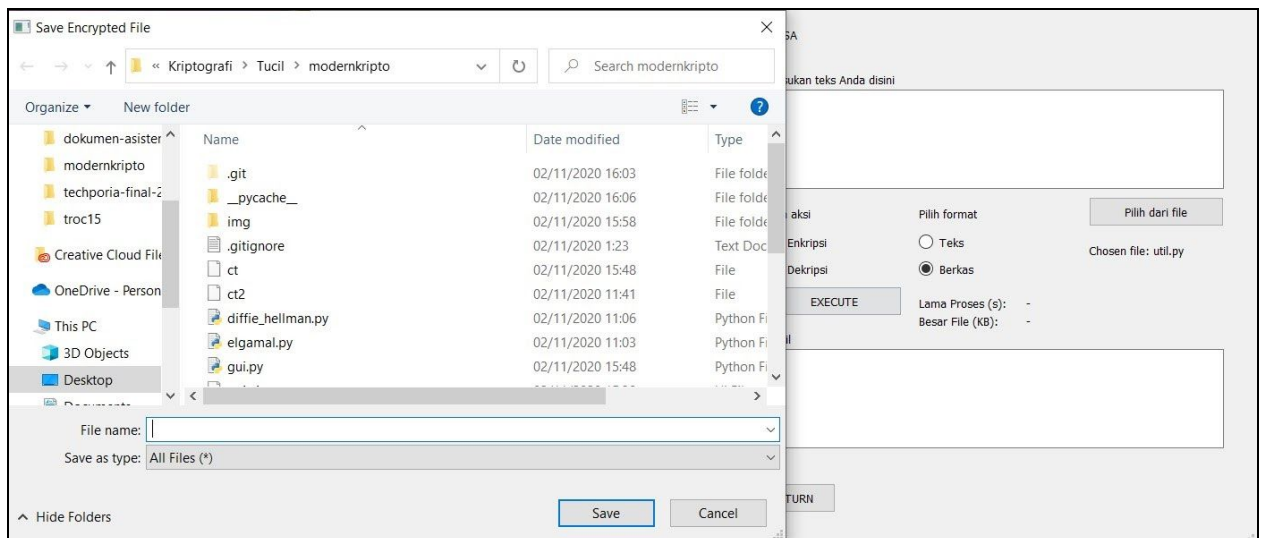
- **Import Key from External File**



- **Get Plaintext from External File**



- **Save Ciphertext to External File**



- **Pembangkitan Kunci Sesi**

MainWindow

RSA

Masukan teks Anda disini

Pilih aksi

☐ Enkripsi

☒ Dekripsi

Pilih format

☐ Teks

☒ Berkas

Pilih dari file

Chosen file: ct

EXECUTE

Lama Proses (s): 4.468827724456787

Besar File (KB): 1.389

Hasil

RETURN

Kunci Kripto Anda

e

d

n

Bangkitkan Kunci

Pilih kunci dari file

Simpan Kunci

Kunci Sesi Anda

n

x

g

y

Bangkitkan Kunci Sesi

79519436869211552269

40607778146596381498

89405956593122769

C. Contoh Pengujian

1. Pengujian Algoritma RSA

a. Kasus Uji 1 (Teks)

Plaintext : Hehehe

Ciphertext : YXUV%Es7sf62AUW0Ids"01I 4j

n : 3848768749365668872432144203102431032705759010885511627668775888643495610741

d : 2754633213287887451503811504269823499869988557592168055292029644799276717663

e : 1751936895143735651778015813304681105601271974724791014538620083815686476703

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

p : 67336560354985573680467241513391525153

q : 57157192601993479718128319601872125397

The screenshot shows a Windows application window titled 'MainWindow'. The interface is divided into several sections:

- Kunci Kripto Anda:** Contains three text boxes with values: 'e' (083815686476703), 'd' (644799276717663), and 'n' (888643495610741). Below these are buttons: 'Bangkitkan Kunci', 'Pilih kunci dari file', and 'Simpan Kunci'.
- Kunci Sesi Anda:** Contains three text boxes labeled 'n', 'x', and 'g', and a button 'Bangkitkan Kunci Sesi'.
- RSA Section:**
 - Masukan teks Anda disini:** A large text box containing 'Hehehe'.
 - Pilih aksi:** Radio buttons for 'Enkripsi' (selected) and 'Dekripsi'. A button 'EXECUTE' is below.
 - Pilih format:** Radio buttons for 'Teks' (selected) and 'Berkas'. A button 'Pilih dari file' is to the right.
 - Performance:** Labels 'Lama Proses (s):' (0.01599717140197754) and 'Besar File (KB):' (-).
 - Hasil:** A text box showing the ciphertext: 'YXUV%Es7sf62AUW0Ids"01I 4j'.
 - RETURN:** A button at the bottom.

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 :

45069129025136821484516711636552171725979584215860454877952070358673575571409375633086535767135854173107

d

:189114773051990898819111789967653253264713047348964035556140547388901143688083308053939592528211895154203

e :

274233606793070319711173859452162612357731965655685173497471145993066931367196325799077831624299905285137

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

p : 14230922453268212295229539548456221527818383080826117

q : 19270262183888930679226013069278624933802333070076061

Waktu: 3.68s

Ukuran file eksternal: 0.054 KB

RSA

Masukan teks Anda disini

Pilih aksi

☒ Enkripsi

☐ Dekripsi

Pilih format

☐ Teks

☒ Berkas

Pilih dari file

Chosen file: pt

EXECUTE

Lama Proses (s): 3.6487271785736084

Besar File (KB): 0.054

Hasil

RETURN

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

The screenshot shows a Windows application window titled "MainWindow" with a menu bar and standard window controls. The main area is titled "ELGAMAL" and is divided into several sections. On the left, under "Kunci Kripto Anda", there are input fields for P (1493), x (422), g (244), and y (212), along with buttons for "Bangkitkan Kunci", "Pilih kunci dari file", and "Simpan Kunci". To the right of this, under "Kunci Sesi Anda", there are input fields for n, x, g, and y, with buttons for "Bangkitkan Kunci Sesi" and a large empty text box. The central part of the window has a text input area labeled "Masukan teks Anda disini" containing the text "aku sangat suka tubes". Below this are radio buttons for "Pilih aksi" (Enkripsi is selected, Dekripsi is unselected) and "Pilih format" (Teks is selected, Berkas is unselected), with a "Pilih dari file" button. An "EXECUTE" button is positioned below the action and format selections. To the right of the execute button, it displays "Lama Proses (s): 0.01030707359313" and "Besar File (KB): -". At the bottom, there is a "RETURN" button. The "Hasil" section at the bottom right contains a text box displaying the ciphertext: "(*())VZ(tVA(Z(J((@j(3□:((J(t!".

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

Kunci Kripto Anda

P

257783

x

90554

g

13928

y

95187

Bangkitkan Kunci

Pilih kunci dari file

Simpan Kunci

Kunci Sesi Anda

n

x

g

y

Bangkitkan Kunci Sesi

ELGAMAL

Masukan teks Anda disini

Pilih aksi

☒ Enkripsi
 ☐ Dekripsi

Pilih format

☐ Teks
 ☒ Berkas

Pilih dari file

Chosen file: hihi.txt

EXECUTE

Lama Proses (s): 4.13699626922607

Besar File (KB): 0.158

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 = 3487714286201858443682399759038178706667657896479
g = 4768913970663469645118300086147007548863547

```

x = 48434800303423060871915934944213050471
y = 10069905163020839618401930277944499168

Key: 3108289229465528903152639404311030864133984309552

Kunci Sesi Anda

n 348771428620185844368239975903

x 03423060871915934944213050471

g 69645118300086147007548863547

y 63020839618401930277944499168

Bangkitkan Kunci Sesi

31082892294655289031
52639404311030864133
984309552