

TUGAS 2

KEAMANAN KOMPUTER/KRIPTOGRAFI



DISUSUN OLEH :

KELAS : 5TKKO-G

PRODI : TEKNIK INFORMATIKA

ANGGOTA :

1. 222061 SITTI ROHANI
2. 222047 SARINI
3. 222060 ANDI ULIL AKBAR

UNIVERSITAS DIPA MAKASSAR

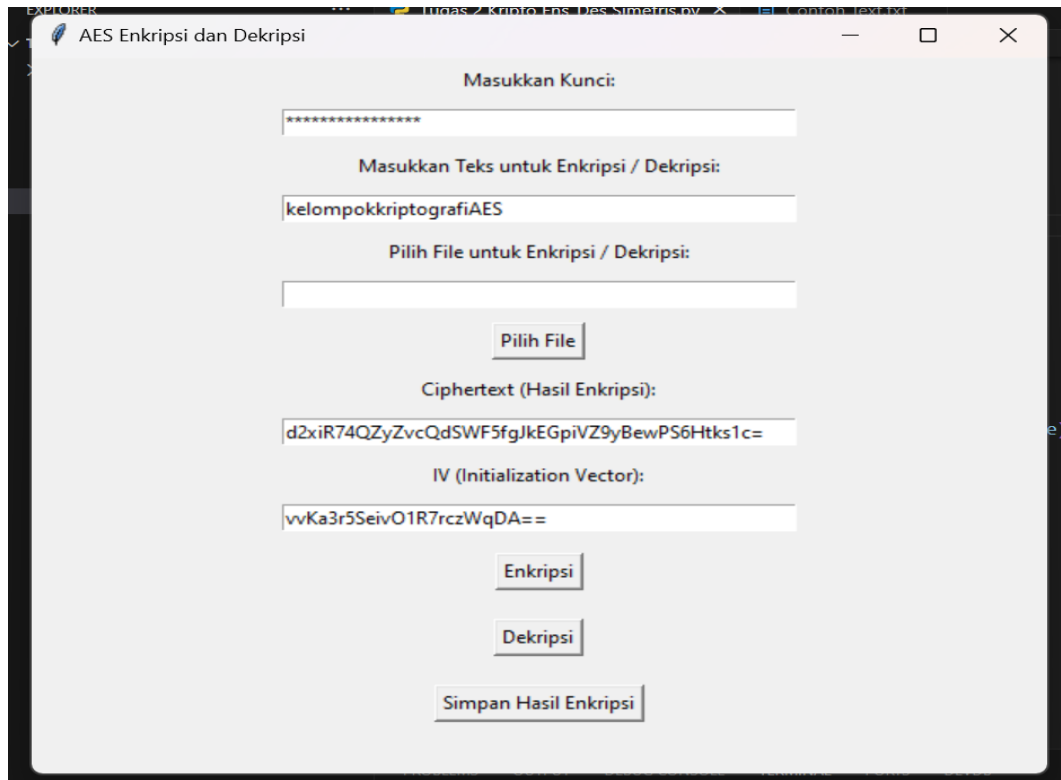
2024/2025

1. SOURCE PROGRAM AES (ADVANCED ENCRYPTION STANDARD)

```
1 import os
2 from tkinter import *
3 from tkinter import messagebox
4 from Crypto.Cipher import AES
5 from Crypto.Util.Padding import pad, unpad
6 from Crypto.Random import get_random_bytes
7 import hashlib
8
9 # Fungsi untuk mengenkripsi data (teks atau file)
10 def encrypt_data(data, key):
11     key = key.encode('utf-8')
12     while len(key) < 32:
13         key += ' '
14     key = key[:32]
15
16     cipher = AES.new(key, AES.MODE_CBC)
17     ct_bytes = cipher.encrypt(pad(data, AES.block_size))
18     iv = hashlib.md5(ct_bytes).hexdigest()
19     ct = base64.b64encode(ct_bytes).decode('utf-8')
20     return iv, ct
21
22 # Fungsi untuk mendekripsi data (teks atau file)
23 def decrypt_data(iv, ct, key):
24     iv = base64.b64decode(iv)
25     ct = base64.b64decode(ct)
26     key = key.encode('utf-8')
27     while len(key) < 32:
28         key += ' '
29     key = key[:32]
30
31     cipher = AES.new(key, AES.MODE_CBC, iv)
32     pt = unpad(cipher.decrypt(ct), AES.block_size)
33     return pt
34
35 # Fungsi untuk memilih file input
36 def choose_file():
37     file_path = filedialog.askopenfilename()
38     if file_path:
39         file_entry.delete(0, END)
40         file_entry.insert(0, file_path)
41
42 # Fungsi untuk mengonversi data (baik file atau teks yang dienkripsi)
43 def on_encrypt():
44     key = key_entry.get()
45     file_path = file_entry.get()
46     text_data = text_entry.get()
47
48     if not key or (not file_path and not text_data):
49         messagebox.showerror("Error", "Kunci atau file/teks belum diisi!")
50         return
51
52     try:
53         if text_data:
54             iv, cipher_text = encrypt_data(text_data.encode('utf-8'), key)
55             result_entry.delete(0, END)
56             result_entry.insert(0, cipher_text)
57             iv_entry.delete(0, END)
58             iv_entry.insert(0, iv)
59         elif file_path:
60             with open(file_path, 'rb') as file:
61                 data = file.read()
62                 iv, cipher_text = encrypt_data(data, key)
63                 result_entry.delete(0, END)
64                 result_entry.insert(0, cipher_text)
65                 iv_entry.delete(0, END)
66                 iv_entry.insert(0, iv)
67
68         save_button.config(state=NORMAL)
69     except Exception as e:
70         messagebox.showerror("Error", f"Terjadi kesalahan: {str(e)}")
71
72 # Fungsi untuk mendekripsi data (baik file atau teks yang dienkripsi)
73 def on_decrypt():
74     key = key_entry.get()
75     cipher_text = result_entry.get()
76     iv = iv_entry.get()
77
78     if not key or not cipher_text or not iv:
79         messagebox.showerror("Error", "Kunci, IV, atau ciphertext tidak diisi!")
80         return
81
82     try:
83         decrypted_data = decrypt_data(iv, cipher_text, key)
84
85         if isinstance(decrypted_data, bytes):
86             try:
87                 decoded_data = decrypted_data.decode('utf-8')
88                 messagebox.showinfo("Sukses", f"Data berhasil di-dekripsi: {decoded_data}")
89             except UnicodeDecodeError:
90                 save_path = filedialog.asksaveasfilename(defaultextension=".bin")
91                 if save_path:
92                     with open(save_path, 'wb') as file:
93                         file.write(decrypted_data)
94                     messagebox.showinfo("Sukses", f"Data biner telah disimpan di {save_path}")
95             except Exception as e:
96                 messagebox.showerror("Error", f"Terjadi kesalahan: {str(e)}")
97
98 # Fungsi untuk menyimpan hasil enkripsi ke file
99 def save_encrypted():
100     cipher_text = result_entry.get()
101     iv = iv_entry.get()
102     if not cipher_text or not iv:
103         messagebox.showerror("Error", "Tidak ada ciphertext untuk disimpan!")
104         return
105
106     save_path = filedialog.asksaveasfilename(defaultextension=".txt")
107     if save_path:
108         try:
109             with open(save_path, 'w', encoding='utf-8') as file:
110                 file.write(f"IV: {iv}\nCiphertext: {cipher_text}")
111             messagebox.showinfo("Sukses", f"Ciphertext telah disimpan di {save_path}")
112         except Exception as e:
113             messagebox.showerror("Error", f"Terjadi kesalahan: {str(e)}")
114
115 # Membuat GUI dengan tkinter
116 root = Tk()
117 root.title("AES (Enkripsi dan Dekripsi)")
118 root.geometry("600x500")
119
120 # Layout
121 Label(root, text="Masukkan Kunci:").pack(pady=5)
122 key_entry = Entry(root, width=50, show="*")
123 key_entry.pack(pady=5)
124
125 # Tampilan Teks
126 Label(root, text="Masukkan teks untuk enkripsi / dekripsi:").pack(pady=5)
127 text_entry = Entry(root, width=50)
128 text_entry.pack(pady=5)
129
130 # Tampilan File
131 Label(root, text="Pilih file untuk enkripsi / dekripsi:").pack(pady=5)
132 file_entry = Entry(root, width=50)
133 file_entry.pack(pady=5)
134 choose_button = Button(root, text="Pilih file", command=choose_file)
135 choose_button.pack(pady=5)
136
137 # Tombol untuk Enkripsi
138 Label(root, text="Ciphertext (Hasil Enkripsi):").pack(pady=5)
139 result_entry = Entry(root, width=50)
140 result_entry.pack(pady=5)
141
142 # Tombol untuk Dekripsi
143 Label(root, text="IV (Initialization Vector):").pack(pady=5)
144 iv_entry = Entry(root, width=50)
145 iv_entry.pack(pady=5)
146
147 # Tombol untuk Enkripsi dan Dekripsi
148 encrypt_button = Button(root, text="Enkripsi", command=on_encrypt)
149 encrypt_button.pack(pady=5)
150
151 decrypt_button = Button(root, text="Dekripsi", command=on_decrypt)
152 decrypt_button.pack(pady=5)
153
154 save_button = Button(root, text="Simpan Hasil Enkripsi", state=DISABLED, command=save_encrypted)
155 save_button.pack(pady=5)
156
157 root.mainloop()
```

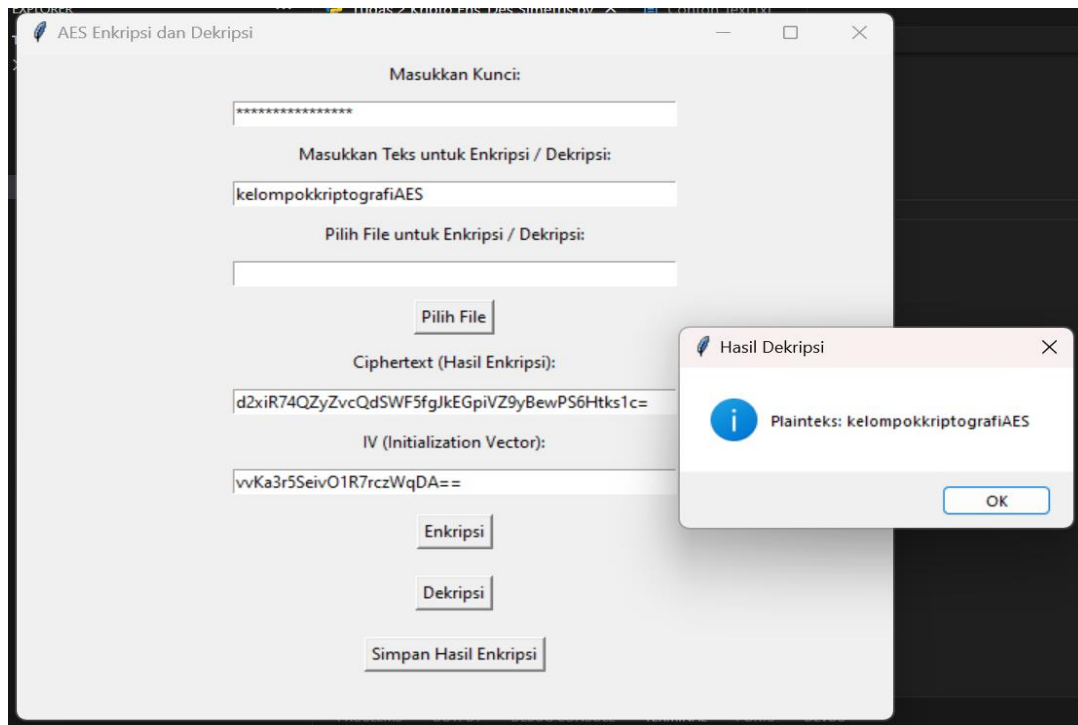
2. TAMPILAN/OUTPUT AES

➤ TAMPILAN TEKS ENSKRIPSI



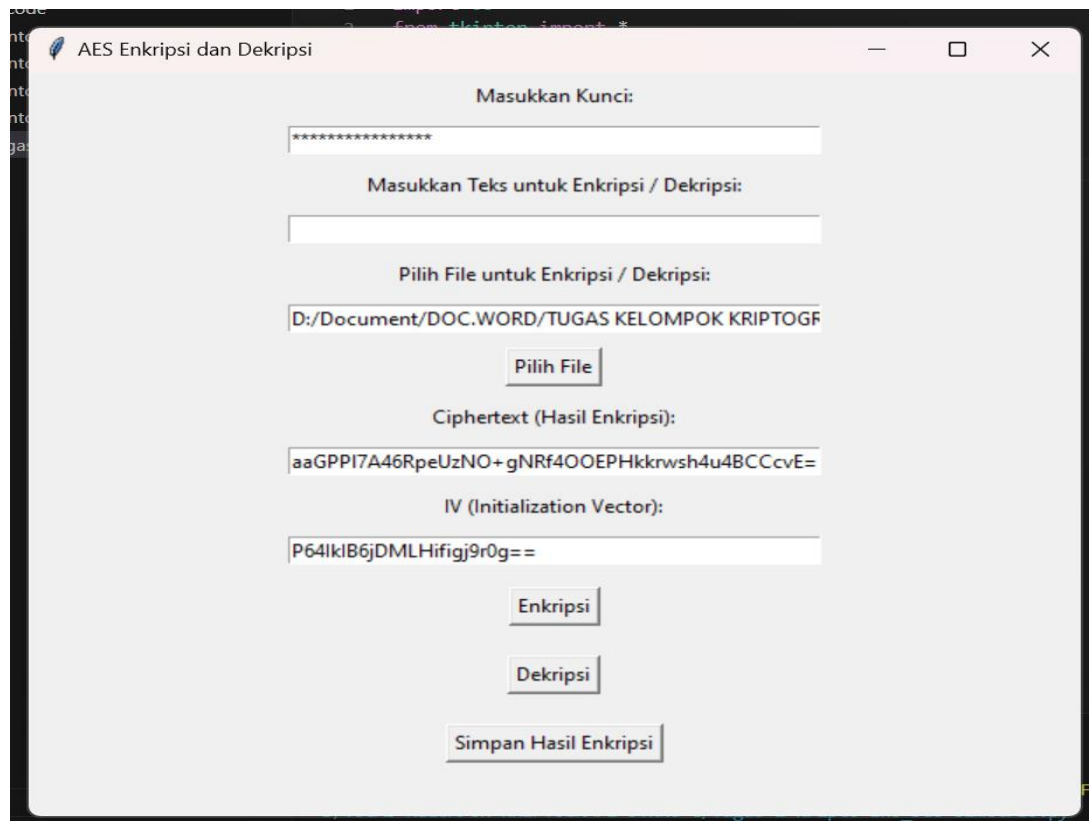
The screenshot shows a window titled "AES Enkripsi dan Dekripsi". It contains several input fields and buttons. The "Masukkan Kunci:" field is filled with "*****". The "Masukkan Teks untuk Enkripsi / Dekripsi:" field is filled with "kelompokkriptografiAES". The "Pilih File untuk Enkripsi / Dekripsi:" field is empty. Below it is a "Pilih File" button. The "Ciphertext (Hasil Enkripsi):" field is filled with "d2xiR74QZyZvcQdSWF5fgJkEGpiVZ9yBewPS6Htks1c=". The "IV (Initialization Vector):" field is filled with "vvKa3r5SeivO1R7rczWqDA==". At the bottom, there are three buttons: "Enkripsi", "Dekripsi", and "Simpan Hasil Enkripsi".

➤ TAMPILAN TEKS DESKRIPSI



The screenshot shows the same "AES Enkripsi dan Dekripsi" window as before, but with the "Dekripsi" button highlighted. A small pop-up window titled "Hasil Dekripsi" is overlaid on the main window. The pop-up contains an information icon and the text "Plainteks: kelompokkriptografiAES". There is an "OK" button at the bottom of the pop-up.

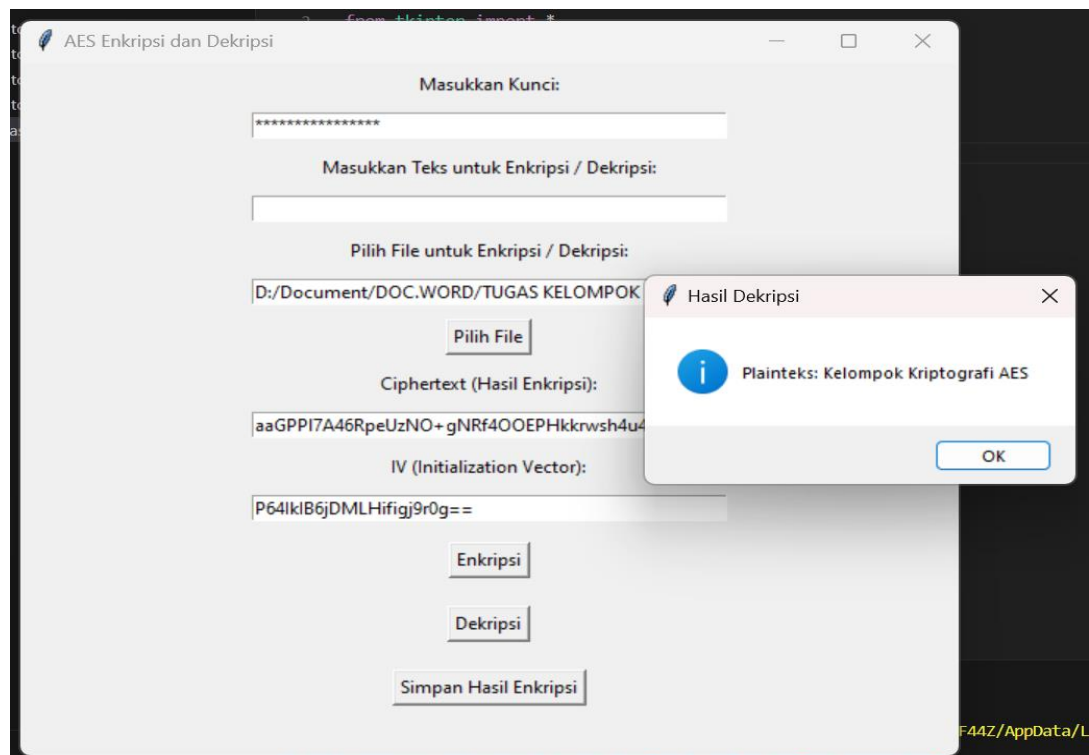
➤ TAMPILAN FILE ENSKRIPSI



The screenshot shows the 'AES Enkripsi dan Dekripsi' application window. It contains the following fields and buttons:

- Masukkan Kunci:** A text input field containing a masked key (*****).
- Masukkan Teks untuk Enkripsi / Dekripsi:** A text input field.
- Pilih File untuk Enkripsi / Dekripsi:** A text input field containing the file path 'D:/Document/DOC.WORD/TUGAS KELOMPOK KRIPTOGF'.
- Pilih File** button.
- Ciphertext (Hasil Enkripsi):** A text input field containing the ciphertext 'aaGPPI7A46RpeUzNO+gNRf4OOEPHkkrwsh4u4BCCcvE='.
- IV (Initialization Vector):** A text input field containing the IV 'P64lkIB6jDMLHifigj9r0g== '.
- Enkripsi** button.
- Dekripsi** button.
- Simpan Hasil Enkripsi** button.

➤ TAMPILAN FILE DESKRIPSI



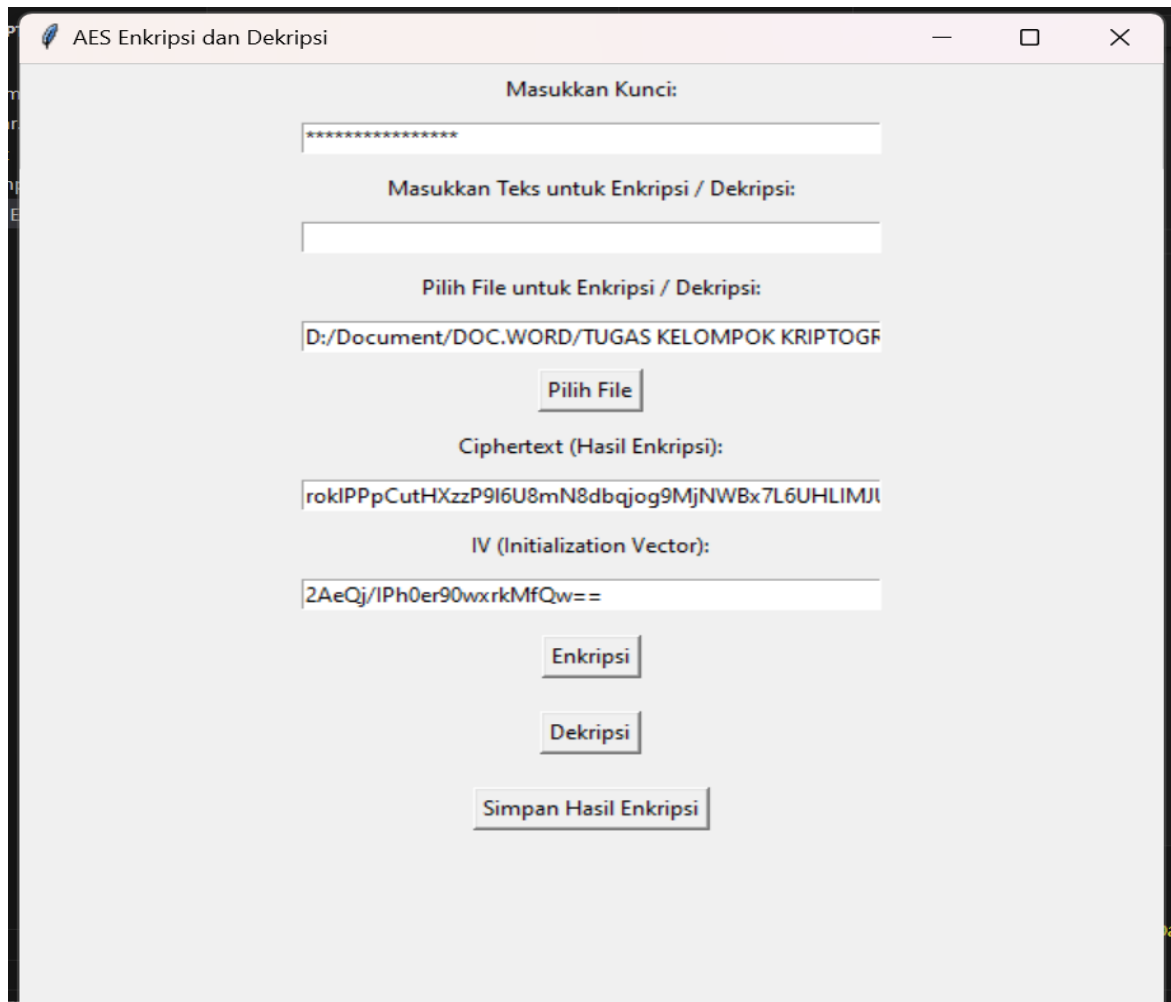
The screenshot shows the 'AES Enkripsi dan Dekripsi' application window with the decryption process. A message box titled 'Hasil Dekripsi' is overlaid on the window.

Hasil Dekripsi message box content:

- Icon: Information (i).
- Text: 'Plainteks: Kelompok Kriptografi AES'.
- Button: 'OK'.

The background application window shows the same fields as the previous screenshot, but the 'Ciphertext (Hasil Enkripsi)' field now contains the same ciphertext as before: 'aaGPPI7A46RpeUzNO+gNRf4OOEPHkkrwsh4u4BCCcvE='.

➤ TAMPILAN GAMBAR ENSKRIPSI



The screenshot shows a window titled "AES Enkripsi dan Dekripsi". It contains several input fields and buttons for encryption and decryption operations.

Masukkan Kunci:

Masukkan Teks untuk Enkripsi / Dekripsi:
[Empty text box]

Pilih File untuk Enkripsi / Dekripsi:
D:/Document/DOC.WORD/TUGAS KELOMPOK KRIPTOGRAFI

Pilih File

Ciphertext (Hasil Enkripsi):
roklPPpCutHXzzP9l6U8mN8dbqjog9MjNWBx7L6UHLIMJl

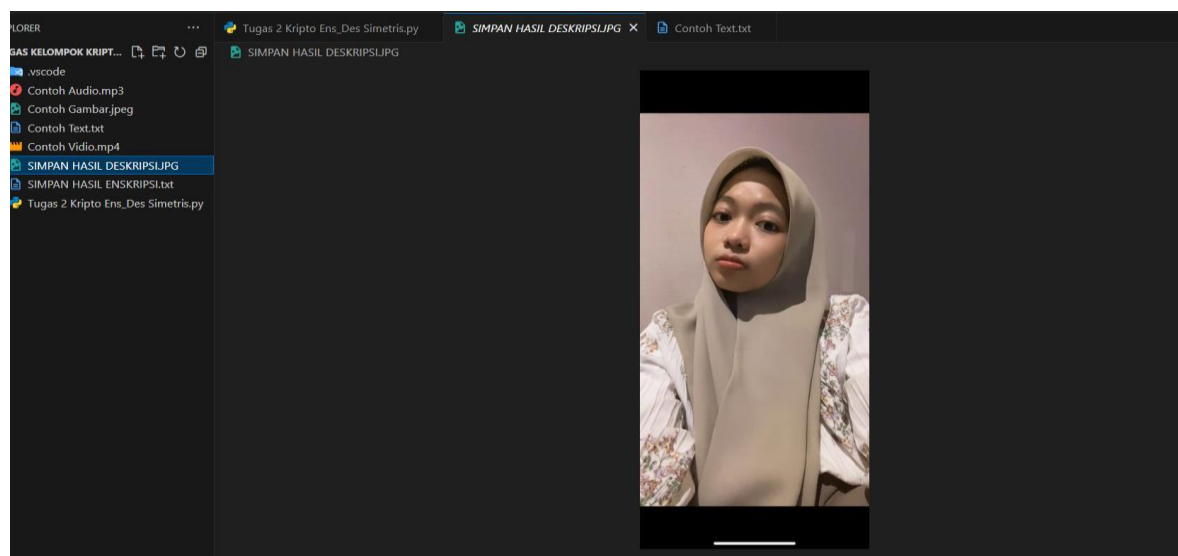
IV (Initialization Vector):
2AeQj/1Ph0er90wxrkMfQw==

Enkripsi

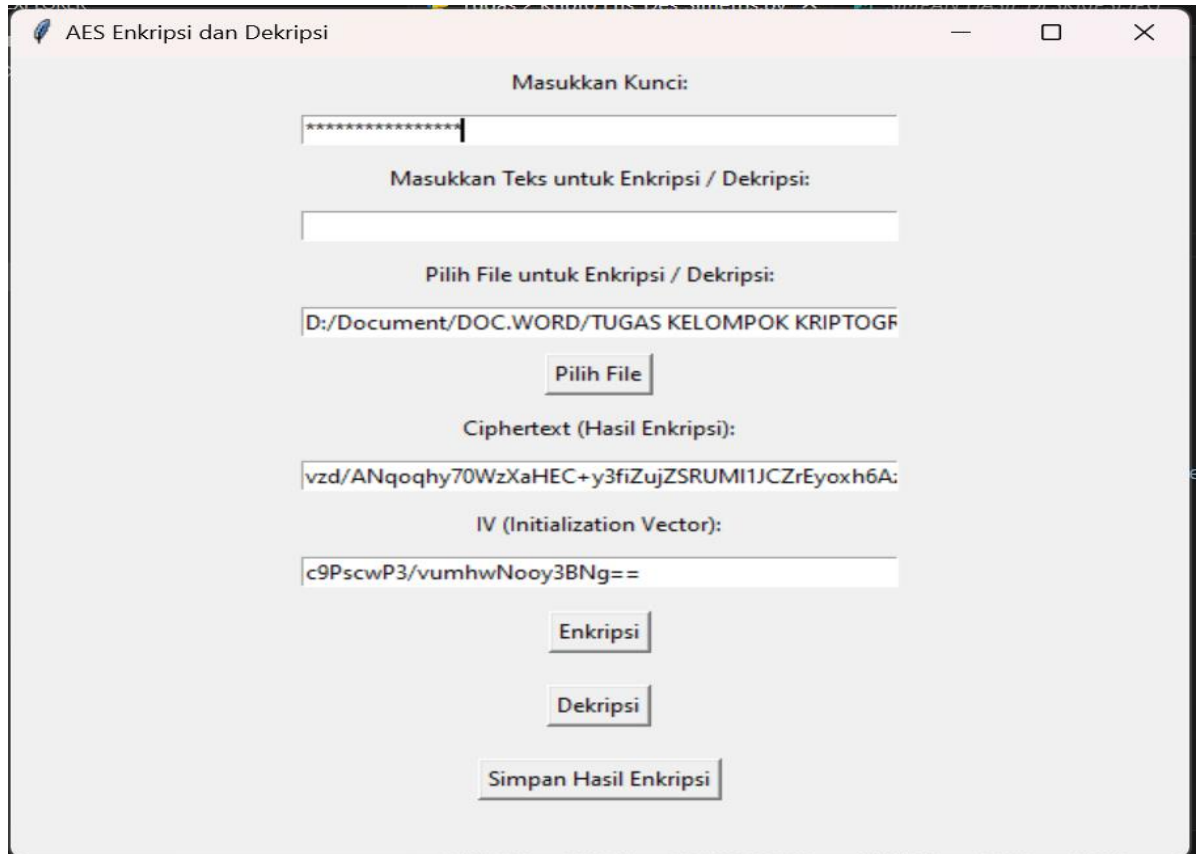
Dekripsi

Simpan Hasil Enkripsi

➤ TAMPILAN GAMBAR DESKRIPSI



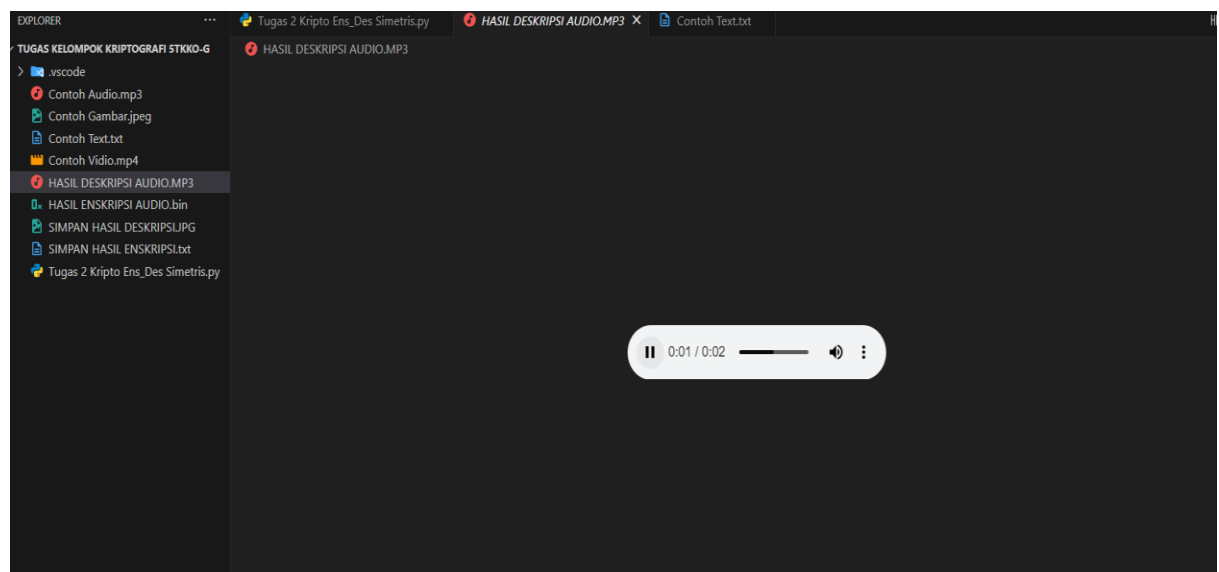
➤ TAMPILAN AUDIO ENSKRIPSI



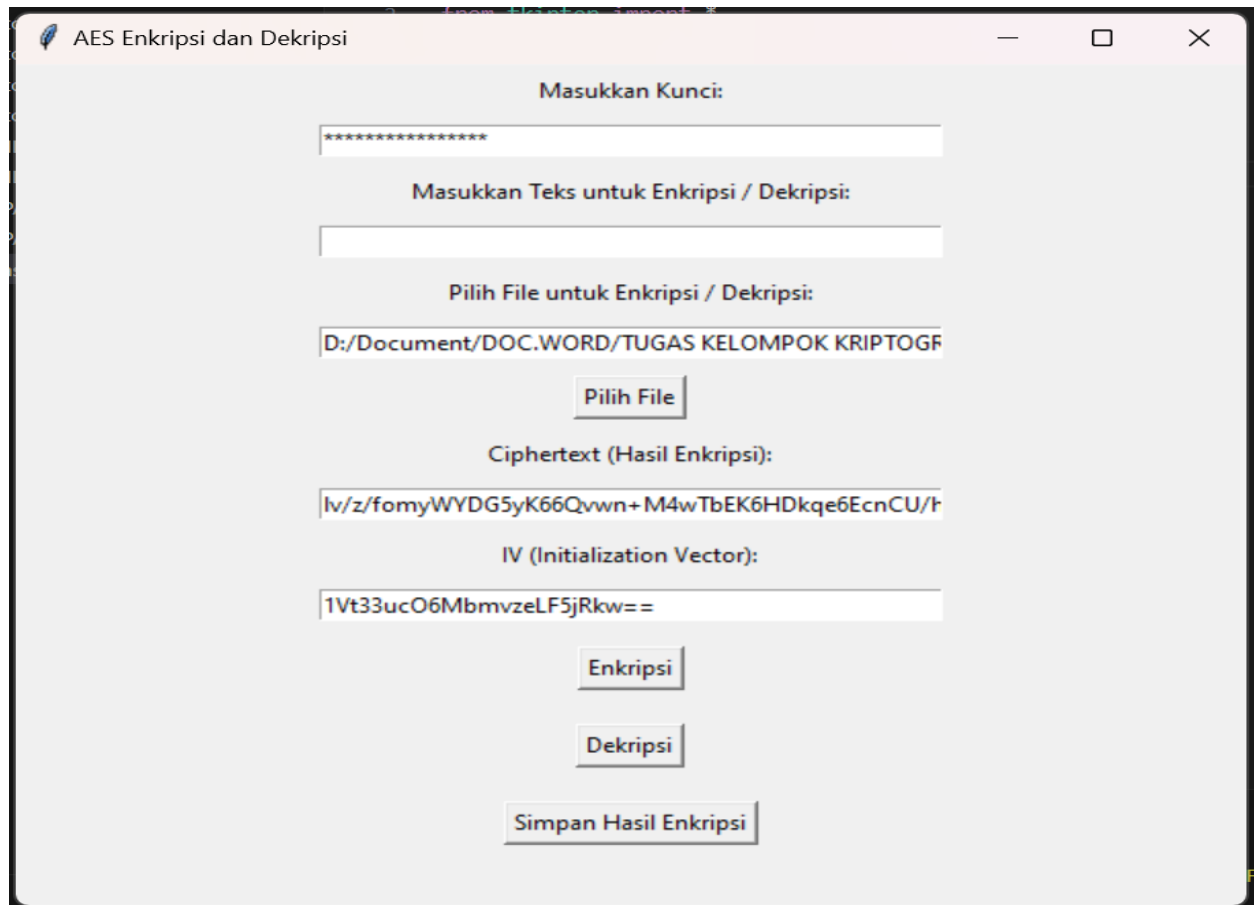
The screenshot shows a web-based application titled "AES Enkripsi dan Dekripsi". It features several input fields and buttons for performing encryption and decryption operations.

- Masukkan Kunci:** A text input field containing a series of asterisks (*****).
- Masukkan Teks untuk Enkripsi / Dekripsi:** A text input field.
- Pilih File untuk Enkripsi / Dekripsi:** A text input field showing the file path "D:/Document/DOC.WORD/TUGAS KELOMPOK KRIPTOGRAFI".
- Pilih File:** A button to select a file.
- Ciphertext (Hasil Enkripsi):** A text input field displaying the ciphertext "vzd/ANqoqhy70WzXaHEC+y3fiZujZSRUMI1JCZrEyoxh6A:". Below this field is a label "IV (Initialization Vector):".
- IV (Initialization Vector):** A text input field displaying the IV "c9PscwP3/vumhwNooy3BNg==".
- Buttons:** "Enkripsi", "Dekripsi", and "Simpan Hasil Enkripsi".

➤ TAMPILAN AUDIO DESKRIPSI



➤ TAMPILAN VIDIO ENSKRIPSI



The screenshot shows a web application interface for AES encryption and decryption. The title bar reads "AES Enkripsi dan Dekripsi". The interface includes the following elements:

- Masukkan Kunci:** A text input field containing ten asterisks (*****).
- Masukkan Teks untuk Enkripsi / Dekripsi:** An empty text input field.
- Pilih File untuk Enkripsi / Dekripsi:** A text input field containing the file path "D:/Document/DOC.WORD/TUGAS KELOMPOK KRIPTOGRAFI".
- Pilih File:** A button located below the file path input.
- Ciphertext (Hasil Enkripsi):** A text input field containing the ciphertext "lv/z/fomyWYDG5yK66Qvwn+M4wTbEK6HDkqe6EcnCU/t".
- IV (Initialization Vector):** A text input field containing the IV "1Vt33ucO6MbmvezLF5jRkw==".
- Enkripsi:** A button for performing encryption.
- Dekripsi:** A button for performing decryption.
- Simpan Hasil Enkripsi:** A button for saving the encryption result.

➤ TAMPILAN VIDIO DESKRIPSI

