

Tugas 1
IF4020 Kriptografi



Oleh:

Willy Wilsen

13520160

Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung
2022/2023

Tampilan Antarmuka Program

Tugas 1 IF4020 Kriptografi

Input

Text

Text

Input plain text

Method

Vigenere Cipher

Key

Input key

Encrypt Decrypt

Result

Download Result

Gambar 1.1 Tampilan Antarmuka Program

Pada program tugas 1 IF4020 Kriptografi, disediakan form untuk melakukan enkripsi dan dekripsi pada suatu *file* atau pesan yang diketik. Form terdiri dari jenis input yang dipilih, metode, dan key yang akan dimasukkan. Hasil enkripsi atau dekripsi akan ditampilkan pada kolom Result.

Contoh plainteks dan cipherteks

Vigenere Cipher

Enkripsi	Dekripsi
----------	----------

Plain: thisplaintext
Key: sony
Cipher: LVVQHZNGFHRVL

Tugas 1 IF4020 Kriptografi

Input

Text

Text

thisplaintext

Method

Vigenere Cipher

Key

sony

Encrypt

Decrypt

Result

LVVQHZNGFHRVL

Download Result

Cipher: LVVQHZNGFHRVL
Key: sony
Plain: THISPLAINTEXT

Tugas 1 IF4020 Kriptografi

Input

Text

Text

LVVQHZNGFHRVL

Method

Vigenere Cipher

Key

sony

Encrypt

Decrypt

Result

THISPLAINTEXT

Download Result

Auto-Key Vigenere Cipher

Enkripsi	Dekripsi
Plain: negara penghasil minyak mentah di dunia Key: INDO Cipher: VRJOEEVEEGWEFOSMAVJMSZCNDMLQB DBQQD	Cipher: VRJOEEVEEGWEFOSMAVJMSZCNDMLQB DBQQD Key: INDO negara penghasil minyak mentah di dunia Plain: NEGARAPENGHASILMINYAKMENTAHDIDU NIA

Tugas 1 IF4020 Kriptografi

Input

Text

Text

negara penghasil minyak mentah di dunia

Method

Auto-Key Vigenere Cipher

Key

INDO

Encrypt

Decrypt

Result

VRJOEEVEEGWEOFOSMAVJMSZCNDMLQBDBQQD

Download Result

Tugas 1 IF4020 Kriptografi

Input

Text

Text

VRJOEEVEEGWEOFOSMAVJMSZCNDMLQBDBQQD

Method

Auto-Key Vigenere Cipher

Key

INDO negara penghasil minyak mentah di dunia

Encrypt

Decrypt

Result

NEGARAPENGHASILMINYAKMENTAHDIDUNIA

Download Result

Extended Vigenere Cipher

Enkripsi	Dekripsi
Plain: gambar1.jpeg Key: Gambar Cipher: [ENCRYPTED] gambar1.jpeg	Cipher: [ENCRYPTED] gambar1.jpeg Key: Gambar Plain: [DECRYPTED] gambar1.jpeg

Tugas 1 IF4020 Kriptografi

Input

File

File

Choose File gambar1.jpeg

Method

Extended Vigenere Cipher

Key

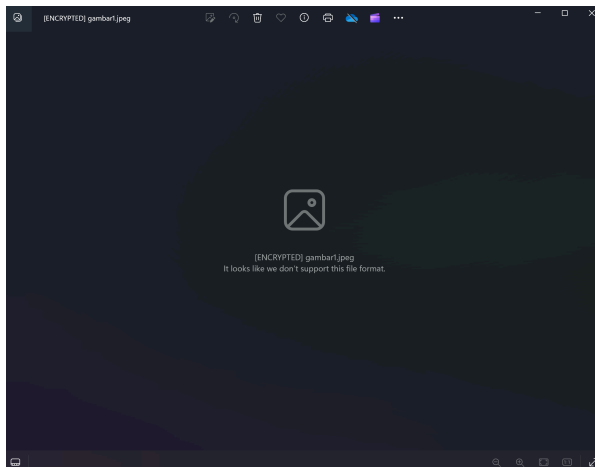
Gambar

Encrypt Decrypt

Result

File has been encrypted in output/[ENCRYPTED] gambar1.jpeg

Download Result



Tugas 1 IF4020 Kriptografi

Input

File

File

Choose File [ENCRYPTED] gambar1.jpeg

Method

Extended Vigenere Cipher

Key

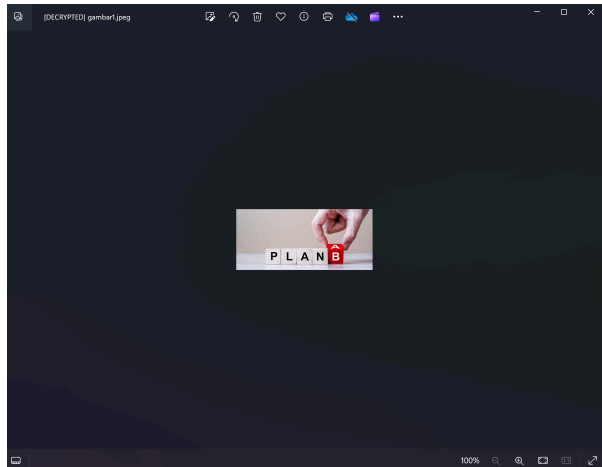
Gambar

Encrypt Decrypt

Result

File has been decrypted in output/[DECRYPTED] gambar1.jpeg

Download Result



Playfair Cipher

Enkripsi	Dekripsi
Plain: temui ibu nanti malam Key: JALAN GANESHA SEPULUH	Cipher: ZBR SFYKUPGLGRKVS NLQV Key: JALAN GANESHA SEPULUH

Cipher: ZBRSFYKUPGLGRKVSNLQV

Tugas 1 IF4020 Kriptografi

Input

Text

Text

temui ibu nanti malam

Method

Playfair Cipher

Key

JALAN GANESHA SEPULUH

Encrypt Decrypt

Result

ZBRSFYKUPGLGRKVSNLQV

Download Result

Plain: TEMUIIBUNANTIMALAM

Tugas 1 IF4020 Kriptografi

Input

Text

Text

ZBRSFYKUPGLGRKVSNLQV

Method

Playfair Cipher

Key

JALAN GANESHA SEPULUH

Encrypt Decrypt

Result

TEMUIIBUNANTIMALAM

Download Result

Affine Cipher

Enkripsi	Dekripsi
Plain: krypto Key m: 7 Key b: 10 Cipher: CZOLNE	Cipher: CZOLNE Key m: 7 Key b: 10 Plain: KRIPTO

Tugas 1 IF4020 Kriptografi

Input

Text

Text

kripto

Method

Affine Cipher

Key

7

10

Encrypt

Decrypt

Result

CZOLNE

Download Result

Tugas 1 IF4020 Kriptografi

Input

Text

Text

CZOLNE

Method

Affine Cipher

Key

7

10

Encrypt

Decrypt

Result

KRIPTO

Download Result

Hill Cipher

Enkripsi	Dekripsi
Plain: paymoremoney Matrix Size: 3 Key: 17 17 5 21 18 21 2 2 19 Cipher: LNSHDLEWMTRW	Cipher: LNSHDLEWMTRW Matrix Size: 3 Key: 17 17 5 21 18 21 2 2 19 Plain: PAYMOREMONEY

Tugas 1 IF4020 Kriptografi

Input

Text

Text

PAYMOREMONEY

Method

Hill Cipher

Key

3

17

21

2

17

18

2

5

21

19

Encrypt

Decrypt

Result

LNSHDLEWMTRW

Tugas 1 IF4020 Kriptografi

Input

Text

Text

LNSHDLEWMTRW

Method

Hill Cipher

Key

3

17

21

2

17

18

2

5

21

19

Encrypt

Decrypt

Result

PAYMOREMONEY

Super Enkripsi: Extended Vigenere Cipher dan Cipher Transposisi

Enkripsi	Dekripsi
Plain: audio1.mp3 Key Vigenere: Audio Key Transposisi: 3 Cipher: [ENCRYPTED] audio1.mp3	Cipher: [ENCRYPTED] audio1.mp3 Key Vigenere: Audio Key Transposisi: 3 Plain: [DECRYPTED] audio1.mp3

Tugas 1 IF4020 Kriptografi

Input

File

File

Choose File audio1.mp3

Method

Super Enkripsi

Key

Audio

3

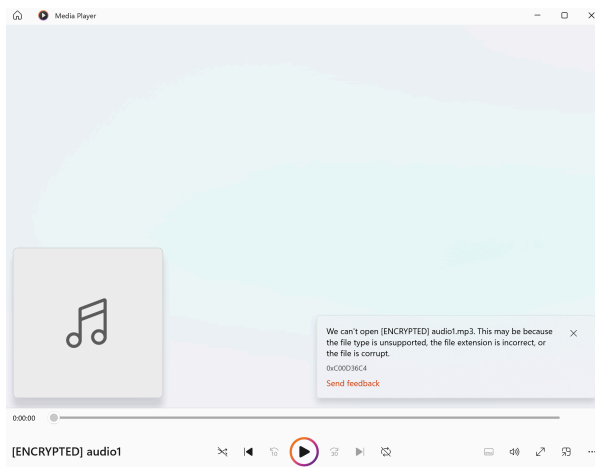
Encrypt

Decrypt

Result

File has been encrypted in output/[ENCRYPTED] audio1.mp3

Download Result



Tugas 1 IF4020 Kriptografi

Input

File

File

Choose File [ENCRYPTED] audio1.mp3

Method

Super Enkripsi

Key

Audio

3

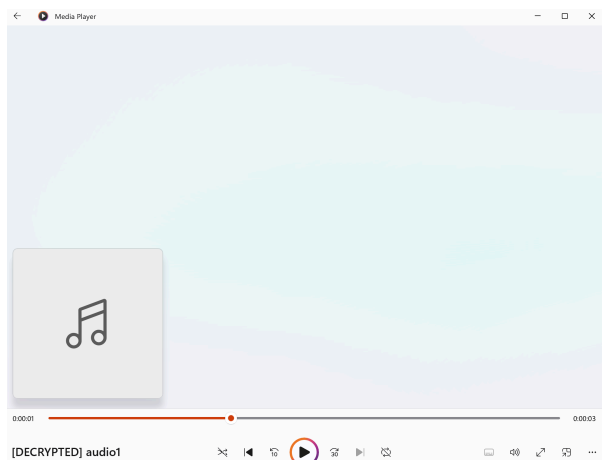
Encrypt

Decrypt

Result

File has been decrypted in output/[DECRYPTED] audio1.mp3

Download Result



Link Github

Link github: <https://github.com/WillyWilsen/Tugas1-Kriptografi>

No	Spek	Berhasil (✓)	Kurang Berhasil (✓)	Keterangan
1.	<i>Vigenere Cipher</i> standard (26 huruf alfabet)	✓		Berhasil
2.	Varian <i>Vigenere Cipher</i> standard (26 huruf alfabet): <i>Auto-Key Vigenere Cipher</i>	✓		Berhasil
3.	<i>Extended Vigenere Cipher</i> (256 karakter ASCII)	✓		Berhasil
4.	<i>Playfair Cipher</i> (26 huruf alfabet)	✓		Berhasil
5.	<i>Affine Cipher</i> (26 huruf alfabet)	✓		Berhasil
6.	<i>Hill Cipher</i> (26 huruf alfabet)	✓		Berhasil
7.	Super Enkripsi	✓		Berhasil
8.	(Bonus) Enigma cipher		✓	Tidak berhasil diimplementasikan
9.	(Bonus) Bahasa Ruby		✓	Berhasil enkripsi atau dekripsi input berupa pesan yang diketik saja