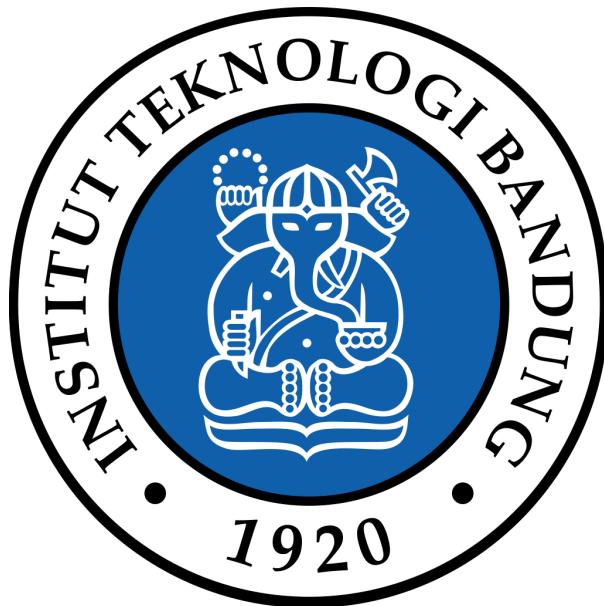


Laporan Tugas 1 IF4020 Kriptografi

Implementasi Algoritma Cipher



Oleh:
Aditya Prawira Nugroho - 13520049
Nathanael Santoso - 13520129

TEKNIK INFORMATIKA
SEKOLAH TEKNIK ELEKTRO DAN INFORMATIKA
INSTITUT TEKNOLOGI BANDUNG
2024

Daftar Isi

Daftar Isi

2

Tampilan Antarmuka Program

Ciphers In Ruby

Input type:

Input text:

Cipher type:

Key:

Output text:

Output bytes:

Created by Aditya and Nathanael

Contoh Plainteks dan Cipherteks

1. Vigenere Cipher Standard

a. Input/Output Plainteks

Ciphers In Ruby

Input type:

Input text:

Cipher type:

Key:

Output text:

Output bytes:

Created by Aditya and Nathanael

Ciphers In Ruby

Input type:

Input text:

Cipher type:

Key:

Output text:

Output bytes:

Created by Aditya and Nathanael

Enkripsi plainteks “Percobaan yang bagus” dengan kunci “bermain” dengan bentuk output plainteks dan base64

Ciphers In Ruby

Input type:

Input text:

Cipher type:

Key:

Output text:

Output bytes:

Created by Aditya and Nathanael

Dekripsi dari cipherteks “qioojnbrpmnoobkle” dengan kunci “bermain”

b. Input/Output File Teks “input.txt”

Ciphers In Ruby

Input type:

Input file:

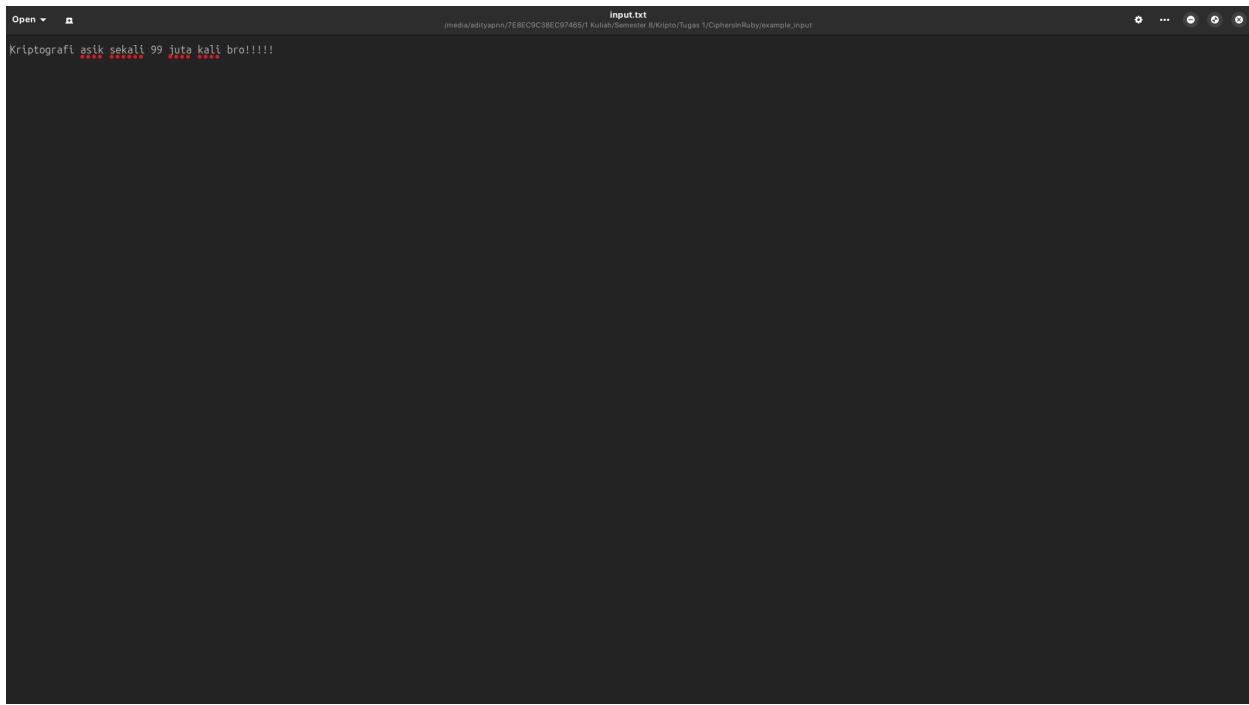
Cipher type:

Key:

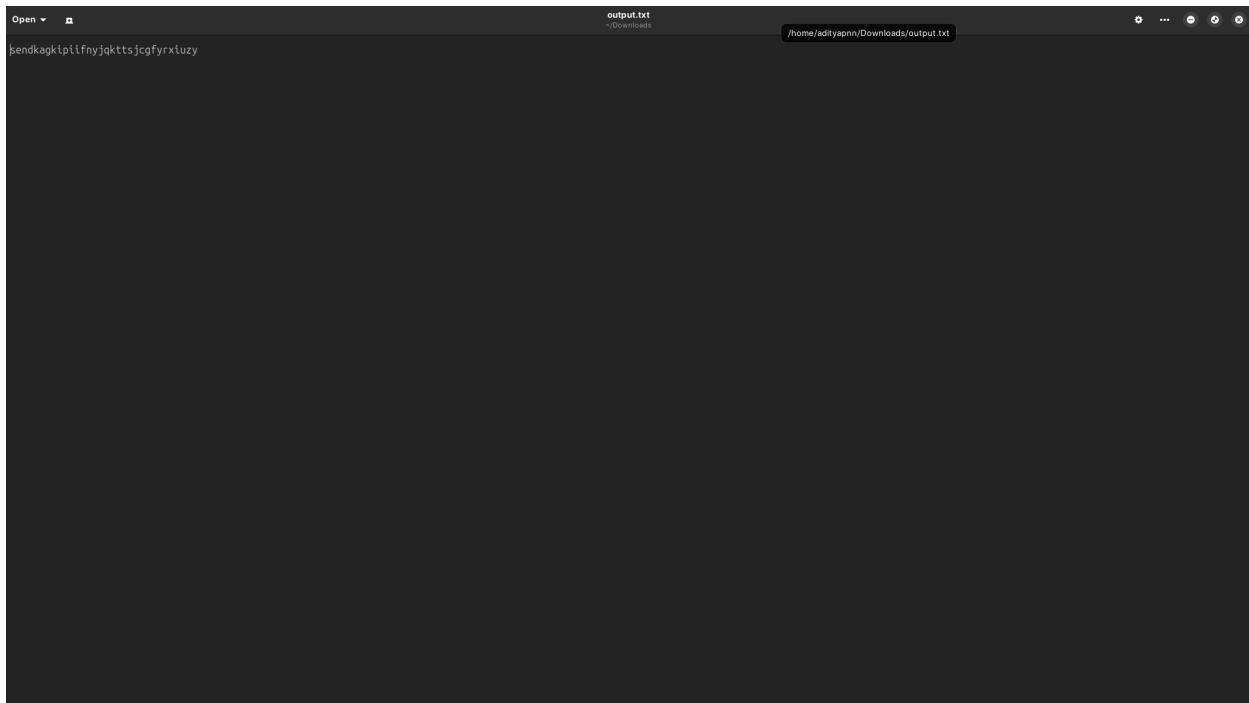
Output text:

Output bytes:

Created by Aditya and Nathanael



```
Kriptografi asik sekali 99 juta kali bro!!!!
```



```
jsendkagkipiifnyjqkttscgfyrxluzy
```

Hasil enkripsi isi dari file “input.txt” dalam bentuk plainteks dan file yang diunduh menjadi “output”.txt.

Ciphers In Ruby

Input type:

Input text:

Cipher type:

Key:

Output text:

Output bytes:

Created by Aditya and Nathanael

Hasil dekripsi file “output.txt” menjadi plainteks
“criptografiasekaliutakalibro” yang menghilangkan karakter spesial dan angka.

2. Auto-Key Vigenere Cipher

a. Input/Output Plainteks

Ciphers In Ruby

Input type:

Input text:

Cipher type:

Key:

Output text:

Output bytes:

Created by Aditya and Nathanael

Ciphers In Ruby

Input type:

Input text:

Cipher type:

Key:

Output text:

Output bytes:

Created by Aditya and Nathanael

Hasil enkripsi plainteks “Kalau saja kita bisa pergi ke bulan dan matahari” dengan kunci “bumi” dalam plainteks dan base64

Ciphers In Ruby

Input type:

Input text:

Cipher type:

Key:

Output text:

Output bytes:

Created by Aditya and Nathanael

Hasil dekripsi plainteks “luxiesljucicalqlaqmjgxovhcveoxlnzdtntaki” dengan kunci “bumikalausajakitabisapergikebulandanmata”

b. Input/Output File Teks “input.txt”

Ciphers In Ruby

Input type: **Text**

Input text:

Cipher type: **Auto-Key Vigenere**

Key: **bumi**

Output text: **lluxdfogttorsnsswsksdmteitueilrz**

Output bytes: **[108, 108, 117, 120, 109, 102, 111, 183, 116, 116, 111, 114, 115, 110, 115, 115, 119, 115, 107, 107, 109, 109, 116, 117, 101, 105, 116, 117, 101, 105, 108, 114, 122]**

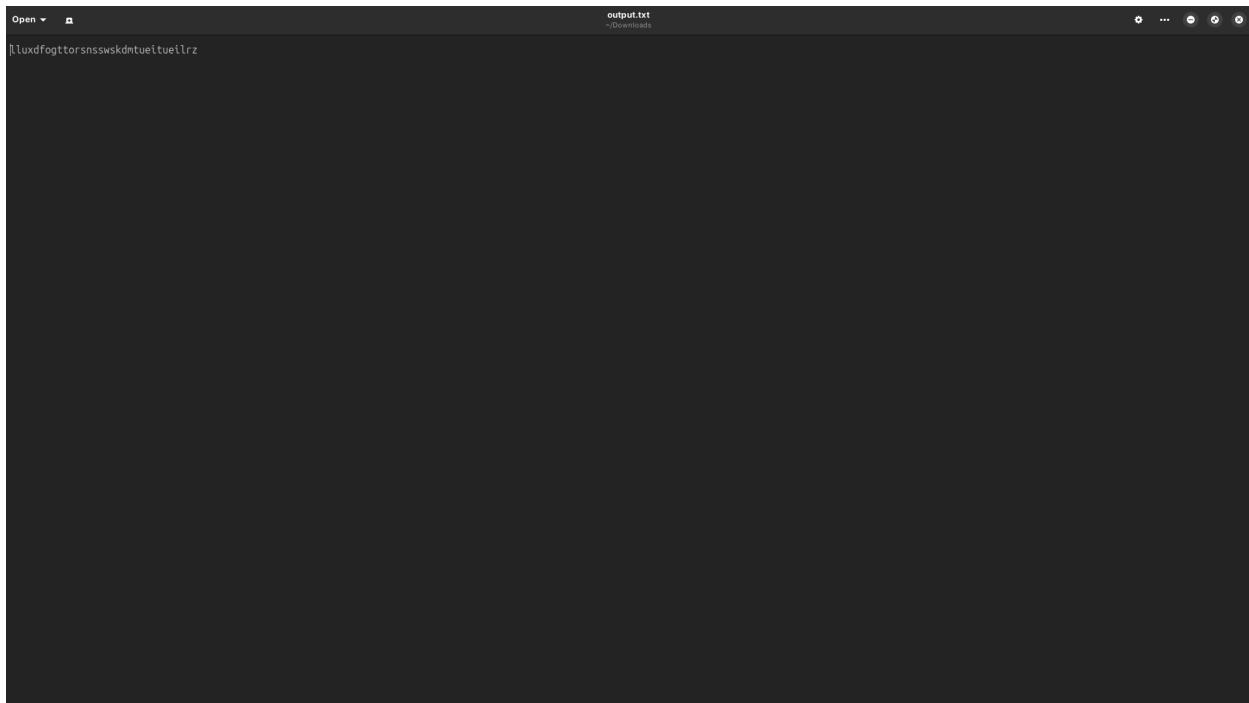
Plaintext Base64

Download Download as binary

Created by Aditya and Nathanael

Open **input.txt** /media/adityaprn/7E8EC9C38ED97465/1 Kuliah/Semester 8/Kripto/Tugas 1/CiphersInRuby/example_input

Kriptografi asik sekali 99 juga kall bro!!!!



Hasil enkripsi *file* dengan kunci “bumi” dalam bentuk file “output.txt”

Ciphers In Ruby

Input type:

Input text:

Cipher type:

Key:

Output text:

Output bytes:

Created by Aditya and Nathanael

Hasil dekripsi *file* “output.txt” dalam bentuk plainteks dengan kunci “bumikriptografiaskekalijutakal”

3. *Playfair Cipher*

a. Input/Output Plainteks

Ciphers In Ruby

Input type:

Input text:

Cipher type:

Key:

Output text:

Output bytes:

Created by Aditya and Nathanael

Ciphers In Ruby

Input type:

Input text:

Cipher type:

Key:

Output text:

Output bytes:

Created by Aditya and Nathanael

Hasil enkripsi plainteks “Attack At Dawn” dengan kunci “Gravity Falls”
dalam plainteks dan base64

Ciphers In Ruby

Input type:

Input text:

Cipher type:

Key:

Output text:

Output bytes:

Created by Aditya and Nathanael

Hasil dekripsi plainteks “gffgbmgfnfaw” dengan kunci “Gravity Falls”

b. Input/Output File Teks “input.txt”

Ciphers In Ruby

Input type:

Input text:

Cipher type:

Key:

Output text:

Output bytes:

Created by Aditya and Nathanael

```
input.txt x ...
CiphersInRuby > example_input > input.txt
1 Kriptografi asik sekali 99 juta kali bro!!!!
2 |
```

```
input.txt output.txt U ...
CiphersInRuby > example_input > output.txt
1 lqbsztetigabyfnqd1momyamzgounmmplz
```

Hasil enkripsi *file* dengan kunci “bumi” dalam bentuk file “output.txt”

Ciphers In Ruby

Input type:

Input text:

Cipher type:

Key:

Output text:

Output bytes:

Created by Aditya and Nathanael

Hasil dekripsi file “output.txt” dalam bentuk plainteks dengan kunci “bumi”, diperhatikan karena algoritma Playfair naturenya lossy maka hasil menjadi “kriptografiasaki sekali xiutaka libro” karena padding dan konversi ‘j’ ke ‘i’.

4. *Affine Cipher*

a. Input/Output Plainteks

Ciphers In Ruby

Input type:

Input text:

Cipher type:

Key:

Output text:

Output bytes:

Created by Aditya and Nathanael

Ciphers In Ruby

Input type:

Input text:

Cipher type:

Key:

Output text:

Output bytes:

Created by Aditya and Nathanael

Hasil enkripsi plainteks “The quick brown fox jumps over 13 lazy dogs.” dengan kunci “fi” atau ($a = 5$, $b = 8$) dalam plainteks dan base64

Ciphers In Ruby

Input type:

Input text:

Cipher type:

Key:

Output text:

Output bytes:

Created by Aditya and Nathanael

Hasil dekripsi plainteks “zrckewsgnpaovhatbeqfuajcplidyxamu” dengan kunci “fi” atau ($a = 5$, $b = 8$)

Ciphers In Ruby

Input type:

Text

Input text:

The quick brown fox jumps over 13 lazy dogs.

Cipher type:

Affine

Key:

ca

Encrypt

Decrypt

Output text:

fvmwiygedzqonpqrbiptcqlmzhaxujqsc

Output bytes:

[102, 118, 109, 119, 105, 121, 103, 101, 100, 122, 113, 111, 110, 112, 113, 114, 98, 105, 107, 116, 99, 113, 108, 109, 122, 104, 97, 120, 117, 106, 113, 115, 99]

Plaintext

Base64

Download

Download as binary

Created by Aditya and Nathanael

Ciphers In Ruby

Input type:

Input text:

Cipher type:

Key:

Output text:

Output bytes:

Created by Aditya and Nathanael

Hasil enkripsi plainteks “The quick brown fox jumps over 13 lazy dogs.” dengan kunci “ca” ($a = 2, b = 0$) dan “ea” atau ($a = 4 b = 0$). Karena kunci invalid, maka program otomatis menyetel kunci valid yaitu “da” atau ($a = 3, b = 0$)

b. Input/Output File Teks “input.txt”

Ciphers In Ruby

Input type:

Input text:

Cipher type:

Key:

Output text:

Output bytes:

Created by Aditya and Nathanael

```
input.txt x ...
CiphersInRuby > example_input > input.txt
1   Kriptografi asik sekali 99 juta kali bro!!!!
2   |
```

```
input.txt output.txt U ...
CiphersInRuby > example_input > output.txt
1   ytsnzkmtujsuwsywgyubsvczuyubsxtk
```

Hasil enkripsi *file* dengan kunci “cumi” dalam bentuk file “output.txt”

Ciphers In Ruby

Input type:

Input text:

Cipher type:

Key:

Output text:

Output bytes:

Created by Aditya and Nathanael

Hasil dekripsi file “output.txt” dalam bentuk plainteks dengan kunci “cumi”.

5. *Hill Cipher*

c. Input/Output Plainteks

Ciphers In Ruby

Input type:

Input text:

Cipher type:

Key:

Output text:

Output bytes:

Created by Aditya and Nathanael

Ciphers In Ruby

Input type:

Input text:

Cipher type:

Key:

Output text:

Output bytes:

Created by Aditya and Nathanael

Hasil enkripsi plainteks “thetruthisoutthere” dengan kunci “hillciph” dalam plainteks dan base64

Ciphers In Ruby

Input type:

Input text:

Cipher type:

Key:

Output text:

Output bytes:

Created by Aditya and Nathanael

Hasil dekripsi plainteks “zvmvnqrbcqwgryrragn” dengan kunci “hillciph”

Ciphers In Ruby

Input type:

Input text:

Cipher type:

Key:

Output text:

Output bytes:

Created by Aditya and Nathanael

Hasil enkripsi plainteks “thetruthisoutther” dengan kunci “hillciph” dalam plainteks untuk menunjukkan padding. Block size yang dipakai adalah 3 dengan random seed 777 untuk padding. Kunci akan di-pad dengan angka seeded random jika tidak mencapai block size kuadrat dan plainteks akan di-pad dengan ‘x’ jika tidak bisa dibagi rata oleh block size.

Ciphers In Ruby

Input type:

Input text:

Cipher type:

Key:

Output text:

Output bytes:

Created by Aditya and Nathanael

Hasil dekripsi plainteks “zvyvnyrbaqwoyrzbcc” dengan kunci “hillciphph” (hasil padding angka seeded random) yang menjadi “thetruthisouttherx” (di-pad “x”)

Ciphers In Ruby

Input type:

Input text:

Cipher type:

Key:

Output text:

Output bytes:

Created by Aditya and Nathanael

Hasil dekripsi plainteks “thetruthisoutthere” dengan kunci “isitreally” yang mengeluarkan invalid key error karena kunci tidak bisa menghasilkan modulo inverse matrix. Dengan kunci seperti ini, enkripsi akan tetap bisa dijalankan, hanya saja plainteks tersebut tidak bisa didekripsi.

d. Input/Output File Teks “input.txt”

Ciphers In Ruby

Input type:

Input text:

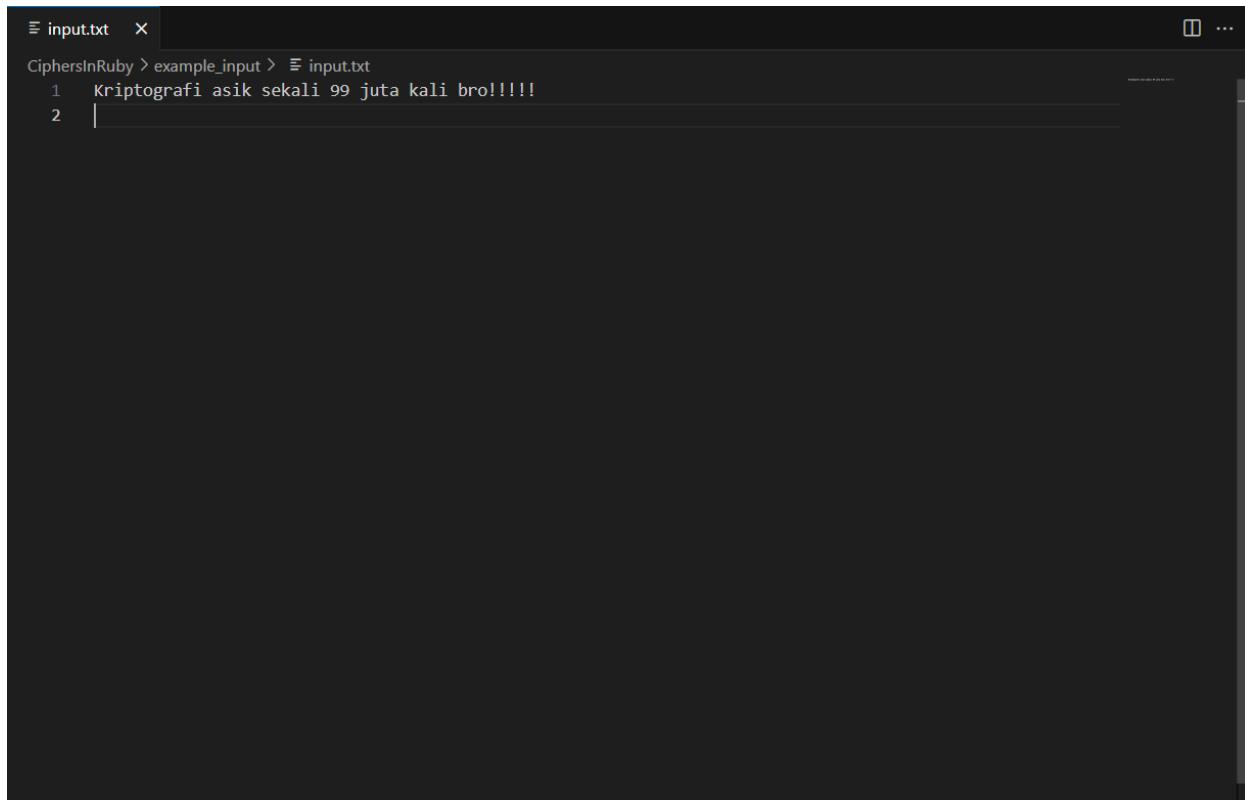
Cipher type:

Key:

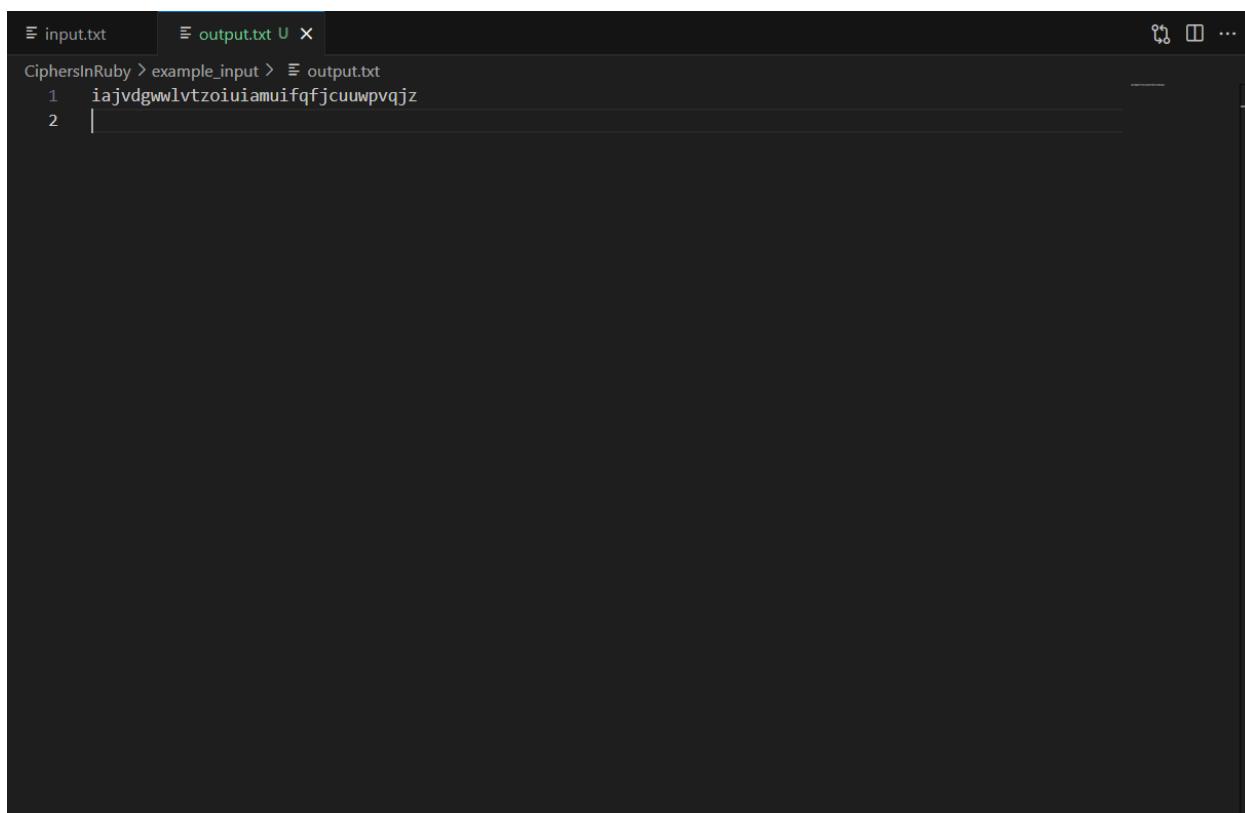
Output text:

Output bytes:

Created by Aditya and Nathanael



```
input.txt
CiphersInRuby > example_input > input.txt
1 Kriptografi asik sekali 99 juga bro!!!!
2 |
```



```
input.txt      output.txt U
CiphersInRuby > example_input > output.txt
1 iajvdgwwlvtzoiuamuifqfjcuuwpvqjz
2 |
```

Hasil enkripsi *file* dengan kunci “hillci” dalam bentuk file “output.txt”

Ciphers In Ruby

Input type:

Input text:

Cipher type:

Key:

Output text:

Output bytes:

Created by Aditya and Nathanael

Hasil dekripsi file “output.txt” dalam bentuk plainteks dengan kunci “hillcihpg” (hasil seeded random padding). Keluaran ada padding ‘x’

6. *Extended Vigenere Cipher*

1. Input/Output Plainteks

Ciphers In Ruby

Input type:

Input text: Bandung adalah ibukota Jawa Barat

Cipher type: Extended Vigenere

Key: semarang

Output text:

Output bytes: [181, 198, 219, 197, 231, 207, 213, 135, 212, 201, 206, 205, 211, 201, 142, 208, 213, 218, 216, 208, 230, 194, 142, 177, 212, 220, 206, 129, 180, 194, 224, 200, 231]

Created by Aditya and Nathanael

Hasil enkripsi “Bandung adalah ibukota Jawa Barat” dengan kunci “semarang”

Ciphers In Ruby

Input type:

Input text: Bandung adalah ibukota Jawa Barat

Cipher type: Extended Vigenere

Key: semarang

Output text:

Output bytes: [66, 97, 110, 100, 117, 110, 103, 106, 97, 100, 97, 108, 97, 104, 15, 105, 98, 117, 107, 111, 110, 97, 15, 74, 97, 119, 97, 32, 66, 97, 114, 97, 116]

Created by Aditya and Nathanael

Hasil dekripsi dari cipherteks menunjukkan karakter yang rusak. Hal ini dikarenakan dalam bahasa Ruby, pembaca byte beberapa karakter spesial didasarkan pada *encoding* “UTF-8” sehingga hasil pembacaan dalam integer melebihi 255 (jumlah karakter ASCII).

2. Input/Output File Teks “input.txt”

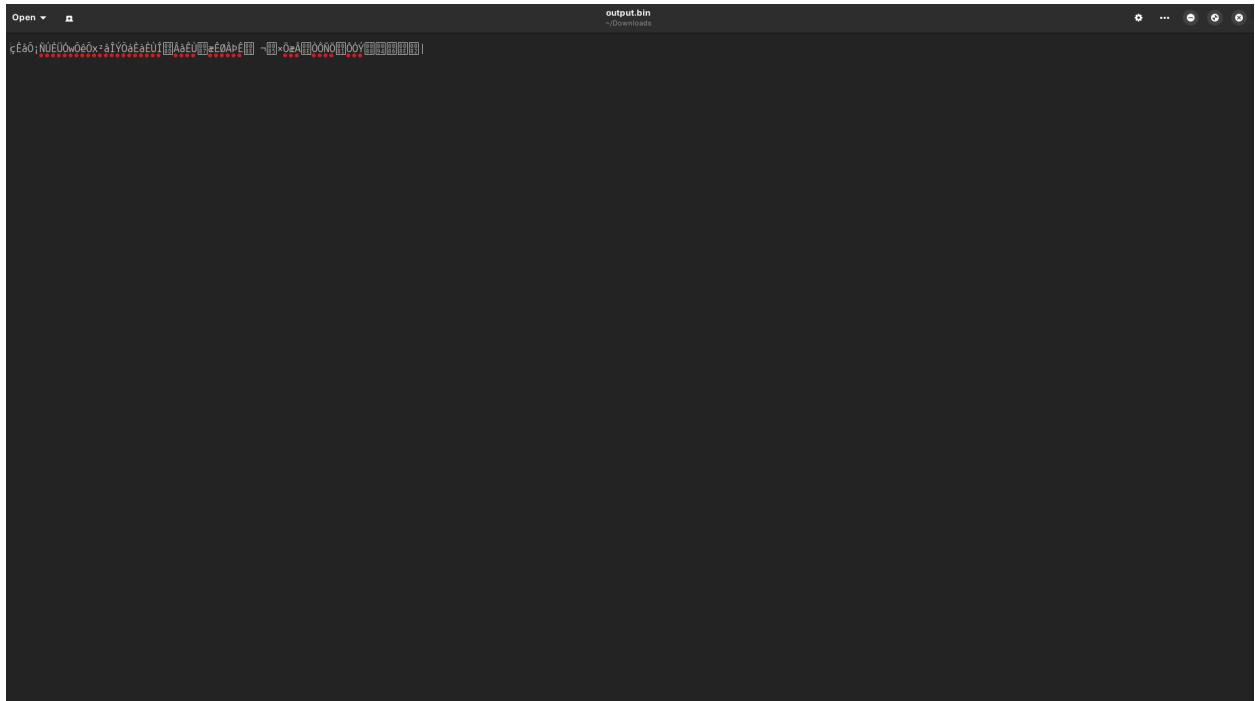
Open       

input.txt
/media/adityapri/7E8EC9C38EC97465/f Kuliah/Geminar B/Kripto/Tugas 1/CiphersInRuby/example_input

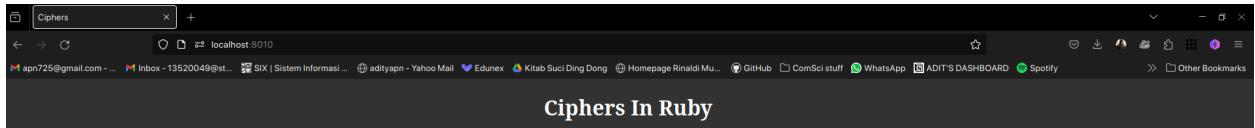
```
Kriptografi asik sekali 99 juta kali bro!!!!  
.....
```

Ciphers In Ruby

Created by Aditya and Nathanael



Hasil enkripsi dengan kunci “semarang” dari file yang diunduh dalam bentuk file *binary*.



Input type:

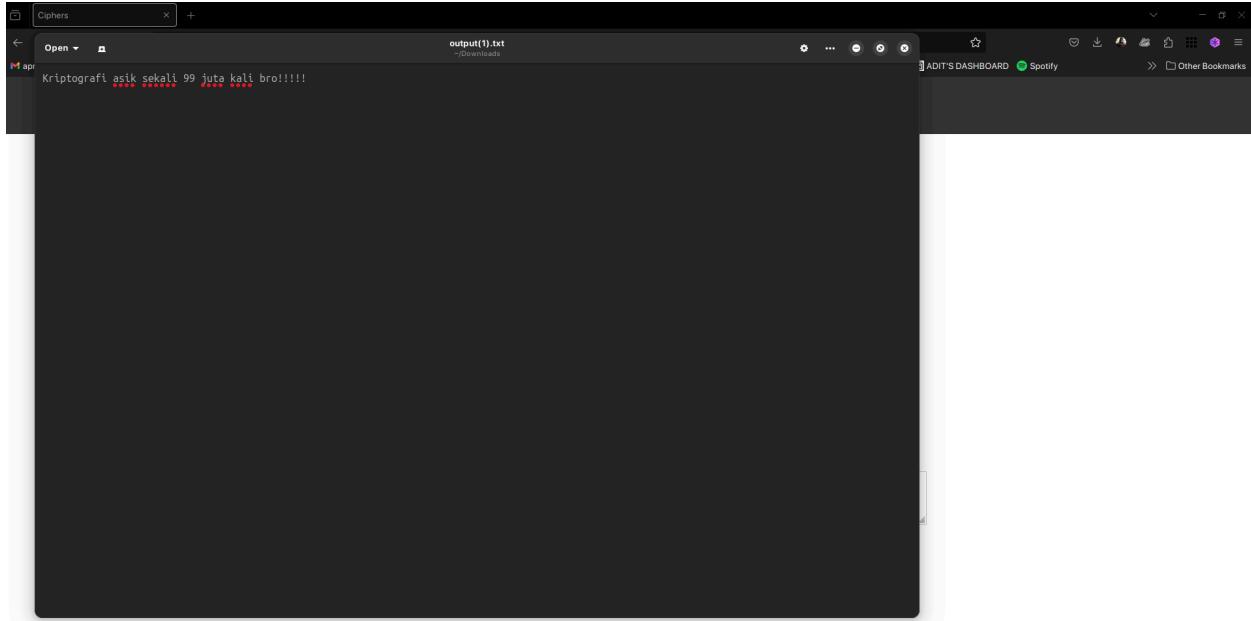
Input text:

Cipher type:

Key:

Output text:

Output bytes:



Created by Aditya and Nathanael

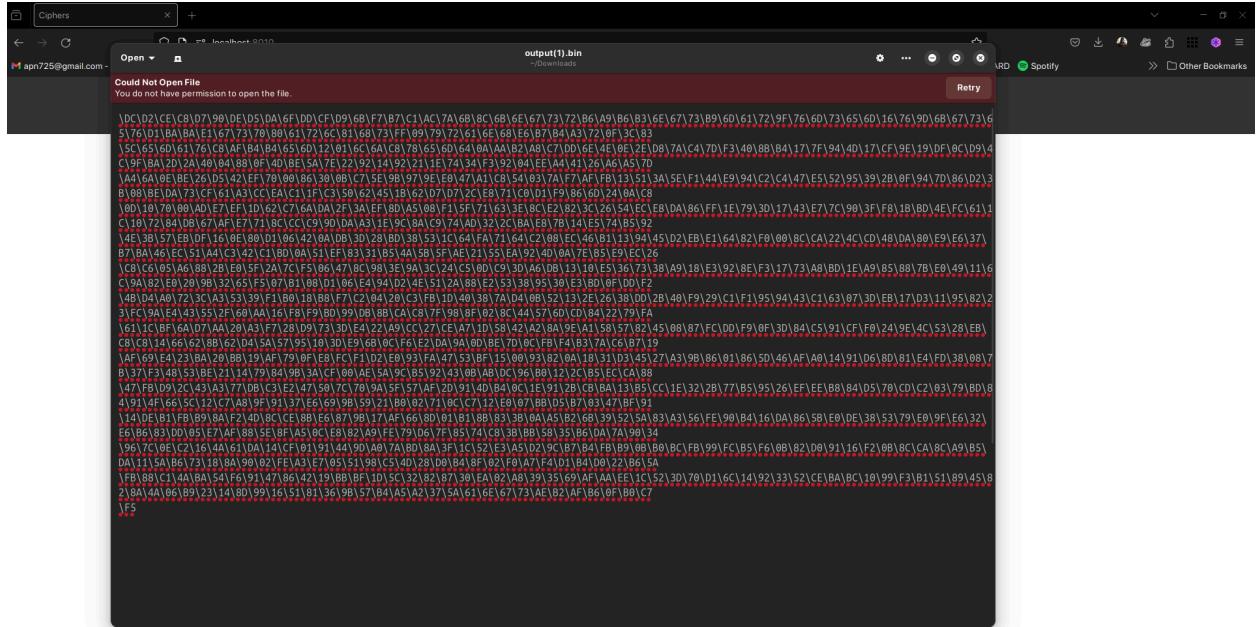
Hasil dekripsi file “output.bin” dengan kunci “semarang” dalam bentuk plainteks dan file semula.

3. Input/Output File Teks “input.png”



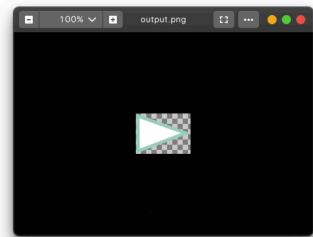
Input type:	<input type="text" value="Text"/>	
Input text:	<input type="text"/>	
Cipher type:	<input checked="" type="radio"/> Extended Vigenere	
Key:	<input type="text" value="semarang"/>	
	<input type="button" value="Encrypt"/> <input type="button" value="Decrypt"/>	
Output text:	<input type="text"/>	
Output bytes:	<pre>[220, 210, 206, 200, 215, 144, 222, 213, 218, 111, 221, 207, 107, 247, 183, 193, 172, 122, 107, 140, 107, 183, 115, 114, 182, 169, 182, 179, 110, 103, 115, 185, 199, 97, 114, 169, 182, 165, 181, 179, 110, 201, 110, 103, 115, 185, 199, 97, 115, 103, 118, 209, 186, 180, 225, 183, 115, 112, 128, 97,</pre>	
Plain text	<input type="button" value="Download"/>	<input type="button" value="Download as binary"/>

Created by Aditya and Nathanael



Created by Aditya and Nathanael

Hasil enkripsi gambar dengan kunci “semarang” dalam bentuk plainteks dan binary.



Created by Aditya and Nathanael

Hasil dekripsi file *binary* dengan kunci “semarang” yang diunduh dengan ekstensi file sesuai dan plainteks.

4. Input/Output File Teks “input.sql”

```

Open ▾
input.sql
+- Database: samplevideo_db
-- Table structure for table 'user_details'

CREATE TABLE IF NOT EXISTS `user_details` (
  `user_id` int(11) NOT NULL AUTO_INCREMENT,
  `username` varchar(255) DEFAULT NULL,
  `first_name` varchar(50) DEFAULT NULL,
  `last_name` varchar(50) DEFAULT NULL,
  `gender` varchar(10) DEFAULT NULL,
  `password` varchar(50) DEFAULT NULL,
  `status` tinyint(10) DEFAULT NULL,
  PRIMARY KEY (`user_id`)
) ENGINE=MyISAM DEFAULT CHARSET=latin1 AUTO_INCREMENT=10001 ;

-- Dumping data for table 'user_details'

INSERT INTO `user_details` ('user_id', 'username', 'first_name', 'last_name', 'gender', 'password', 'status') VALUES
(1, '*****', 'david', 'john', 'Female', '*****', 1),
(2, 'mike20', 'rogers', 'paul', 'Male', '*****', 1),
(3, 'livera92', 'david', 'john', 'Male', '*****', 1),
(4, 'ross95', 'maria', 'sanders', 'Male', '*****', 1),
(5, 'paul85', 'moris', 'miller', 'Female', '*****', 1),
(6, 'smith34', 'daniel', 'michael', 'Female', '*****', 1),
(7, 'james84', 'sanders', 'paul', 'Female', '*****', 1),
(8, 'daniel53', 'mark', 'mike', 'Male', '*****', 1),
(9, 'brooks88', 'morgan', 'maria', 'Female', '*****', 1),
(10, 'morgan65', 'paul', 'miller', 'Female', '*****', 1),
(11, 'sanders84', 'david', 'miller', 'Female', '*****', 1),
(12, 'mariab0', 'christyadon', 'bell', 'Female', '*****', 1),
(13, 'brown71', '*****', 'brown', 'Male', '*****', 1),
(14, 'james63', '*****', 'james', 'Male', '*****', 1),
(15, 'jenny993', 'rogers', 'christian', 'Female', '*****', 1),
(16, 'jones', '*****', 'wright', 'Male', '*****', 1),
(17, 'miller64', 'morgan', 'wright', 'Male', '*****', 1),
(18, 'mark46', 'david', 'ross', 'Female', '*****', 1),

```



Input type:

Text

Input text:

Cipher type:

Extended Vigenere

Key:

File Sgl

Encrypt Decrypt

Output text:

Output bytes:

Plainfile Base64 Download Download as binary

```

$ ./ciphers -o output.bin -k file.sql -t extended_vigenere -d samplevideo_db

```

The terminal output shows the command used to run the cipher tool, followed by the generated binary file 'output.bin'.

Created by Aditya and Nathanael

Hasil enkripsi file input.sql dengan kunci “File Sql” ke dalam bentuk binary dan plainteks



Created by Aditya and Nathanael

Hasil dekripsi file binary dengan kunci “File Sql” dalam bentuk plainteks dan file sql

5. Input/Output File Teks “input.mp3”



Created by Aditya and Nathanael

Hasil enkripsi file mp3 dengan kunci “musik uhuy” dalam bentuk plainteks dan binary



Input type:

Cipher type:

Key:

Output text:

Output bytes:

Encrypt
Decrypt

Plaintext

Base64

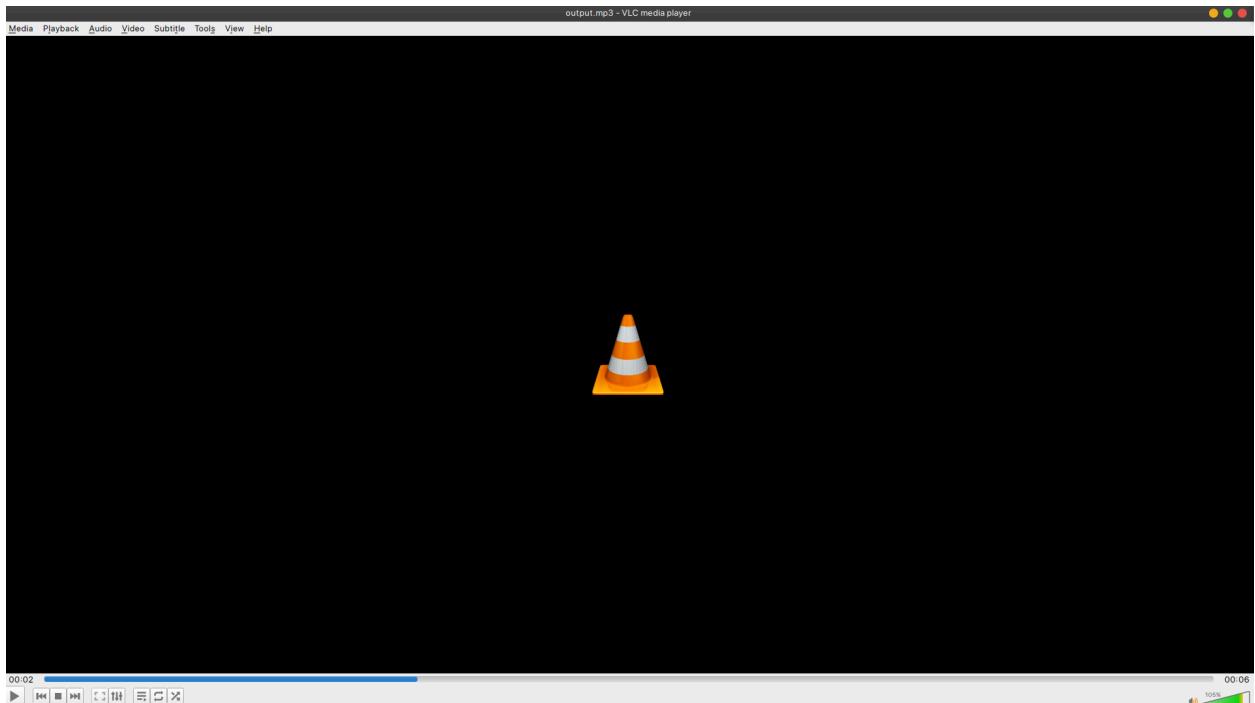
Download

Download as binary

Input text:

Ciphertext:

Created by Aditya and Nathanael



Hasil dekripsi file output(1).bin dengan kunci “musik uhuy” dalam bentuk plainteks dan ekstensi file mp3

6. Input/Output File Teks “input.webm”



Input type: Text

Input text:

Cipher type: Extended Vigenere

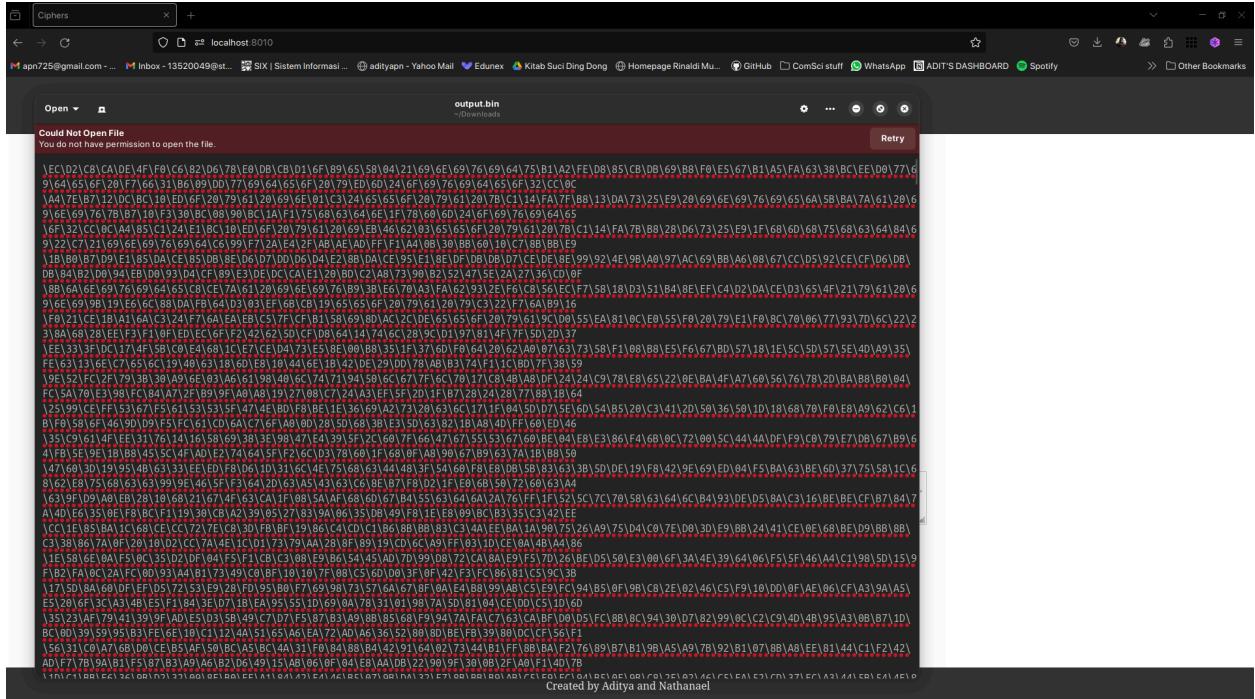
Key: video ya ini

Output text: 10EDp0Mx_0x0ENokexWlinvividusqB_E01_AsgxWc91Dwideo

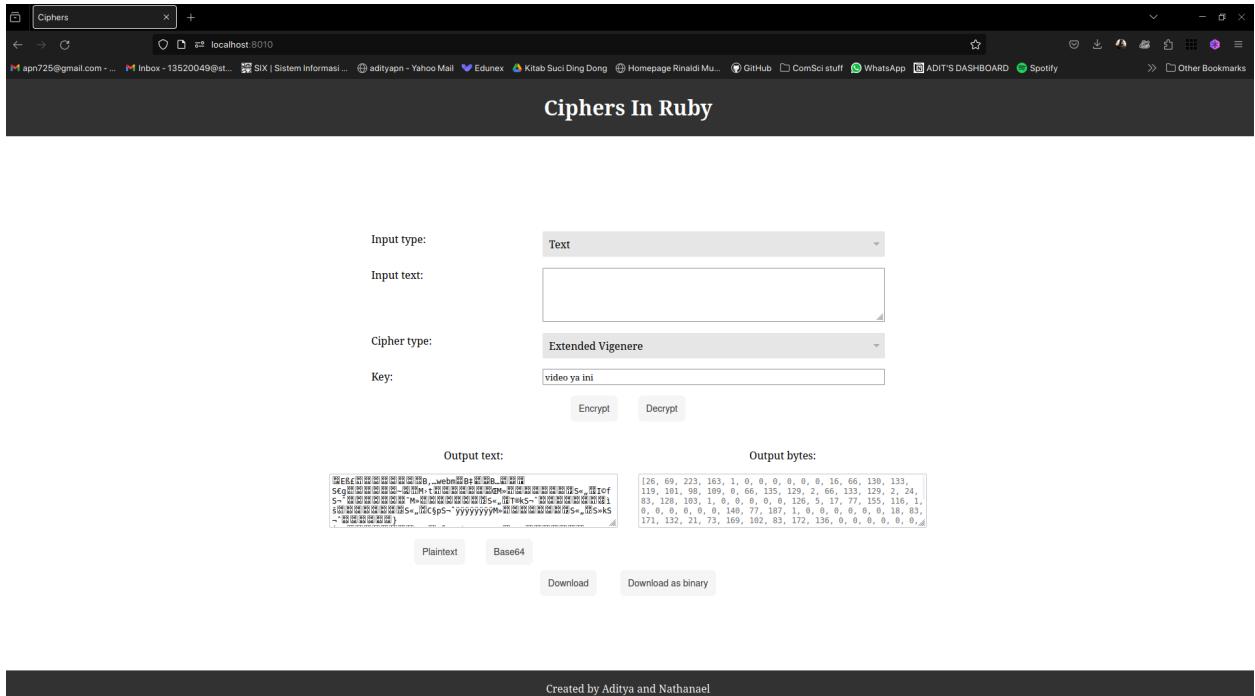
Output bytes: [236, 210, 200, 202, 222, 79, 240, 198, 130, 214, 120, 224, 219, 283, 209, 111, 137, 101, 88, 4, 33, 105, 118, 105, 119, 103, 125, 111, 119, 110, 115, 112, 114, 116, 113, 117, 118, 112, 104, 240, 229, 103, 177, 165, 258, 99, 56, 188, 238, 208, 119, 105, 100, 101, 111, 32, 247, 102, 49, 182, 9, 221, 119, 105]

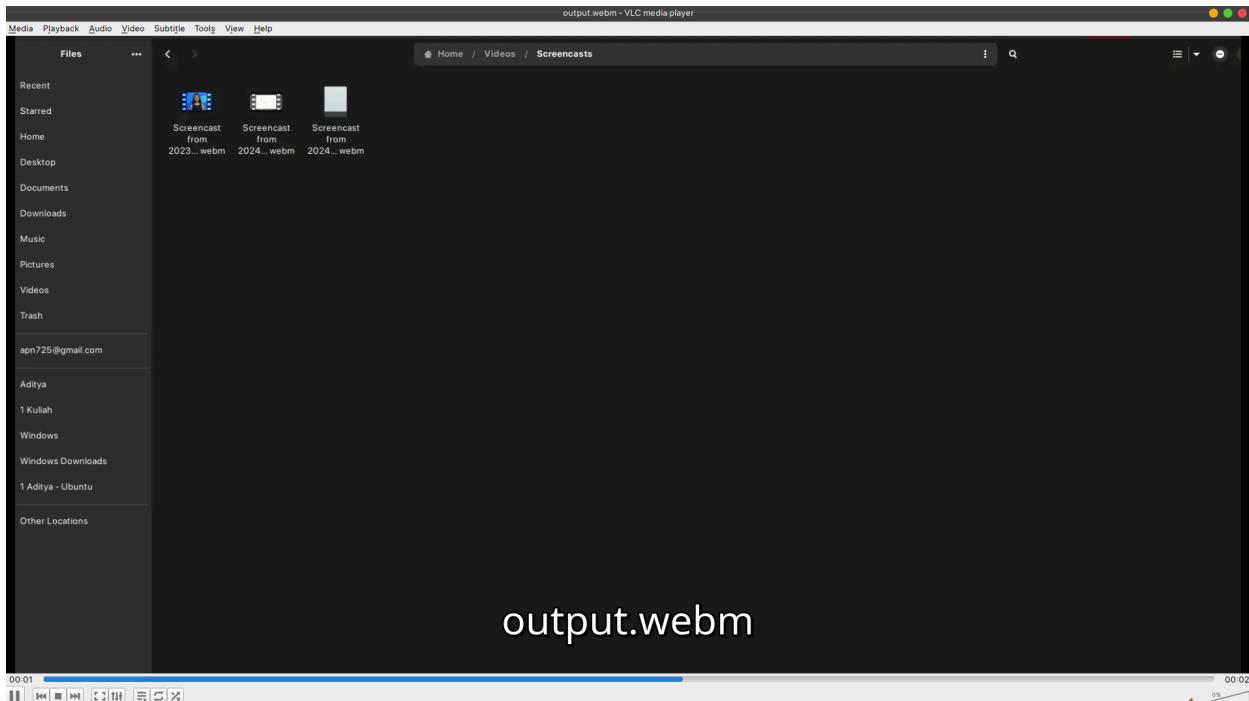
Plaintext Base64

Download Download as binary



Hasil enkripsi file input.webm dengan kunci “video ya ini” dalam bentuk plainteks dan binary.

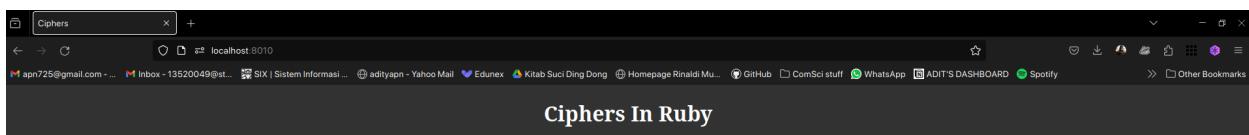




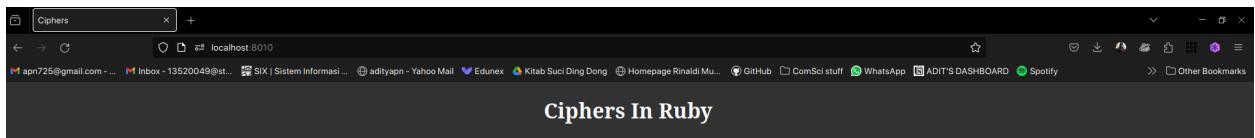
Hasil dekripsi file output.bin dengan kunci “video ya ini” dalam bentuk plainteks dan file ekstensi webm

7. Super Enkripsi

Input/Output Plainteks



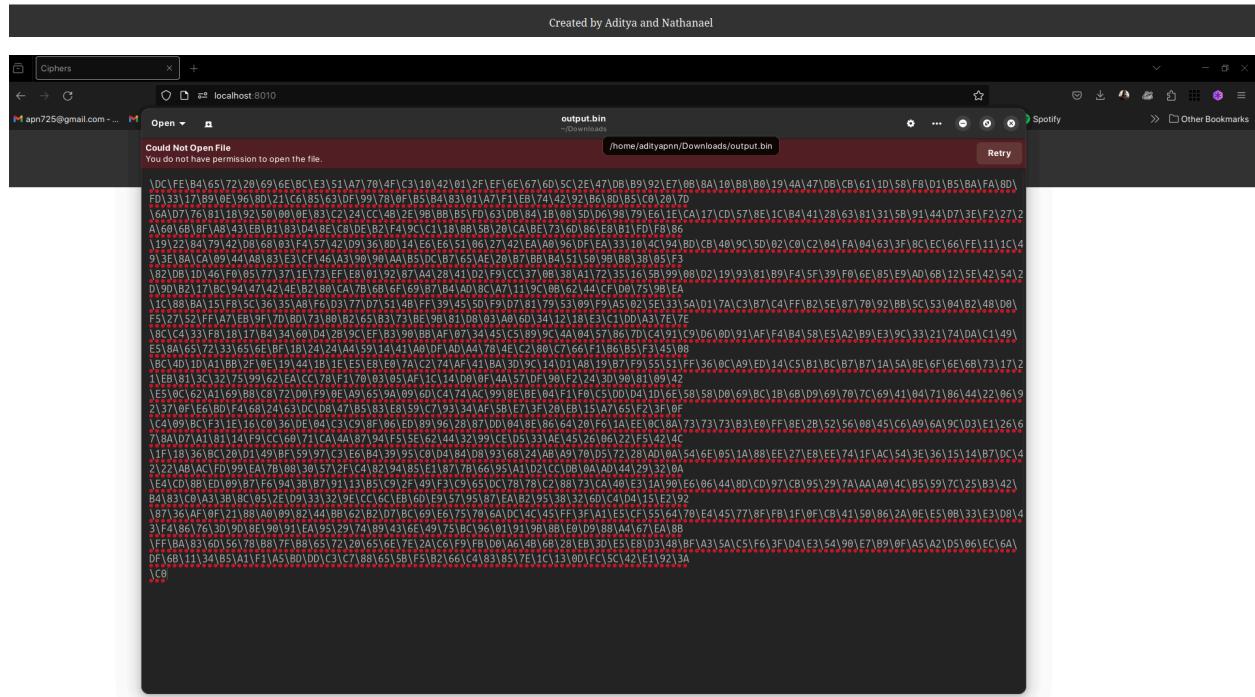
Hasil enkripsi plainteks “melakukanenkripsisuper” dengan kunci “super” dalam bentuk plainteks



Input type:	Text
Input text:	<input type="text" value="åéþþºðþÍåðþðþþþþþþ"/>
Cipher type:	Super Encryption (Extended Vigenere Cipher and Transposition) <input checked="" type="radio"/>
Key:	<input type="text" value="super"/>
	<input type="button" value="Encrypt"/> <input type="button" value="Decrypt"/>
Output text:	<input type="text" value="målukanenkrípsisuper"/>
Output bytes:	[109, 101, 108, 97, 107, 117, 107, 97, 110, 101, 110, 107, 114, 105, 112, 115, 105, 115, 117, 112, 101, 114]
Plaintext	Base64
<input type="button" value="Download"/> <input type="button" value="Download as binary"/>	

Hasil dekripsi plainteks “àéþØ×ØàÙäßÖâØÓáþåÐ×åå” dengan kunci “super” dalam bentuk plainteks

Input/Output File Teks “input.png”



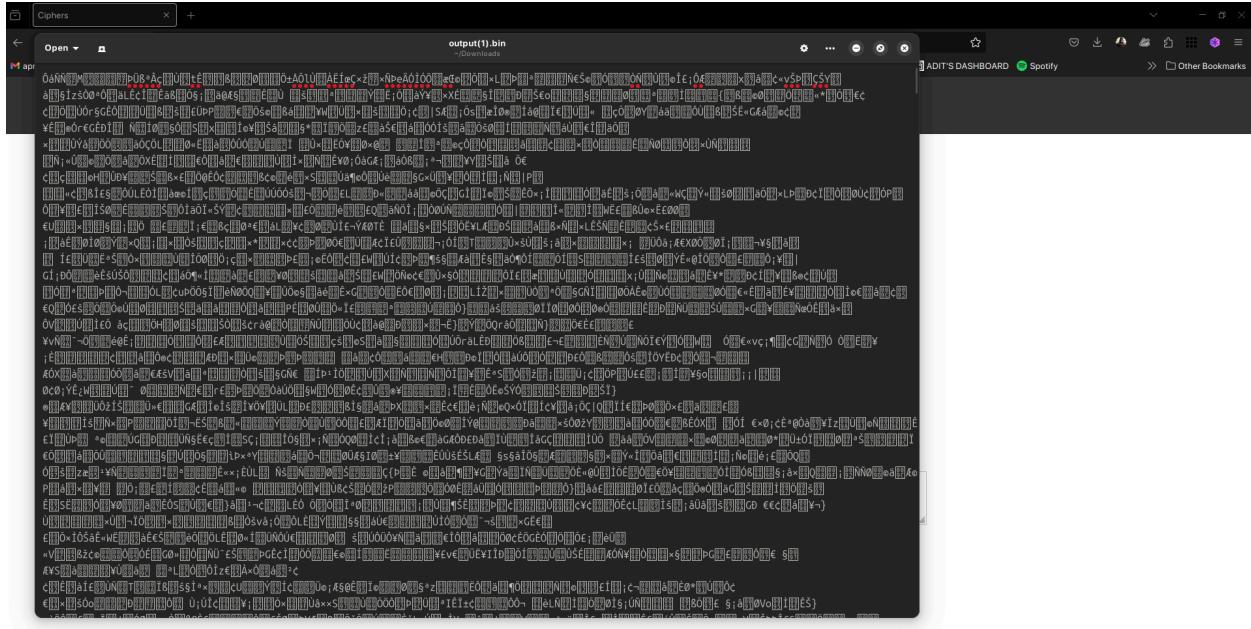
Hasil enkripsi file input.png dengan kunci “super enkripsi” ke dalam bentuk plainteks dan binary

Created by Aditya and Nathanael

Hasil dekripsi file binary dengan kunci “super enkripsi” kembali menjadi file png dan juga dalam bentuk plainteks.

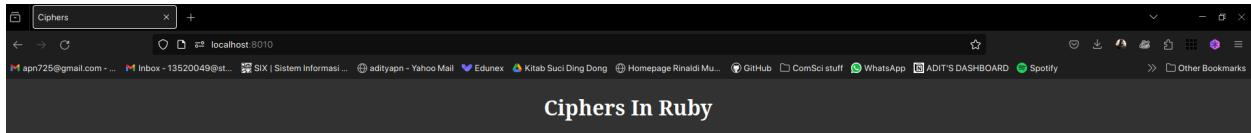
Input/Output File Teks “input.sql”

Created by Aditya and Nathanael



Created by Aditya and Nathanael

Hasil enkripsi file sql dengan kunci “super enkripsi” ke dalam bentuk plainteks dan binary



Ciphers In Ruby

Created by Aditya and Nathanae

```
Ciphers x +  
Mapr Open ⚡  
output.sql  
Mapr  
...  
-- Database: 'samplevideo_db'  
--  
--  
-- Table structure for table 'user_details'  
--  
  
CREATE TABLE IF NOT EXISTS `user_details` (  
    user_id int(11) NOT NULL AUTO_INCREMENT,  
    username varchar(255) DEFAULT NULL,  
    first_name varchar(50) DEFAULT NULL,  
    last_name varchar(50) DEFAULT NULL,  
    gender varchar(10) DEFAULT NULL,  
    password varchar(50) DEFAULT NULL,  
    status tinyint(10) DEFAULT NULL,  
    PRIMARY KEY (`user_id`)  
) ENGINE=MyISAM DEFAULT CHARSET=latin1 AUTO_INCREMENT=100001 ;  
  
-- Dumping data for table 'user_details'  
--  
  
INSERT INTO `user_details` ('user_id', 'username', 'first_name', 'last_name', 'gender', 'password', 'status') VALUES  
(1, 'roger53', 'david', 'john', 'Female', '06a33neu180b07e5c3d74fae02fc65h8', 1),  
(2, '*****', 'rogers', 'paul', 'Male', '*****', 1),  
(3, 'rivera02', 'david', 'John', 'Male', '*****', 1),  
(4, 'rossi', 'maria', 'anders', 'Male', '62f0aa8a4179cd597789760cfc10', 1),  
(5, 'pauls', 'morris', 'miller', 'Female', '61bdd00d07bdfeccca56a5b2b05def', 1),  
(6, 'smith53', 'daniel', 'michael', 'Female', '705553d9f5cb209c26cd7eb6601cd5', 1),  
(7, 'james84', 'anders', 'paul', 'Female', 'bf77f2de092a45b08ed2084c8d1a3573', 1),  
(8, 'daniels53', 'mark', 'mike', 'Male', '299cf71f1d12967408ed200b4e26c1', 1),  
(9, 'brookso5', 'morgan', 'maria', 'Female', 'aa736a35dc15934d67c0a999ccff8f6', 1),  
(10, 'morgan05', 'paul', 'miller', 'Female', 'a280ca31f5a5792e1cefdf1df098569', 1),  
(11, 'sanders84', 'david', 'willie', 'Female', '10c20aef0f08-87a620866175e00f7', 1)
```

Created by Aditya and Nathanael

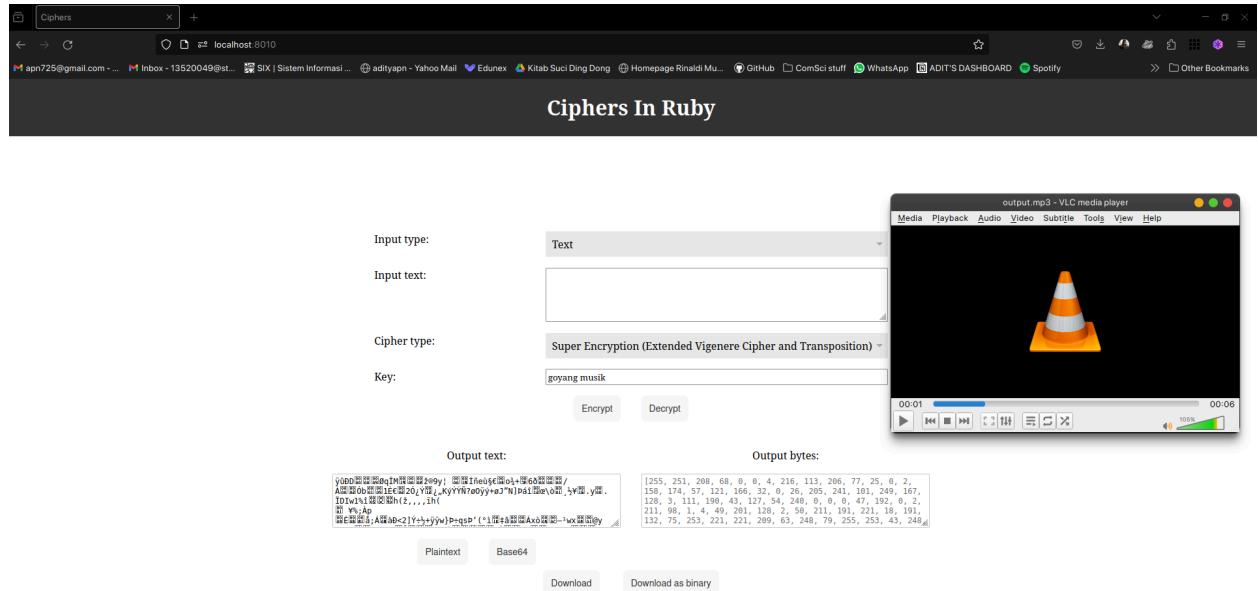
Hasil dekripsi file binary dengan kunci “super enkripsi” ke dalam bentuk plainteks dan juga file sql

Input/Output File Teks “input.mp3”

Ciphers In Ruby

Created by Aditya and Nathanael

Hasil enkripsi file input.mp3 dengan kunci “goyang musik” ke dalam bentuk plainteks dan binary



Hasil dekripsi file binary dengan kunci “goyang musik” ke dalam bentuk plainteks dan mp3 yang dapat dibuka

Input/Output File Teks “input.webm”



Input type: Text

Input text:

Cipher type: Super Encryption (Extended Vigenere Cipher and Transposition)

Key: melihat video

Encrypt Decrypt

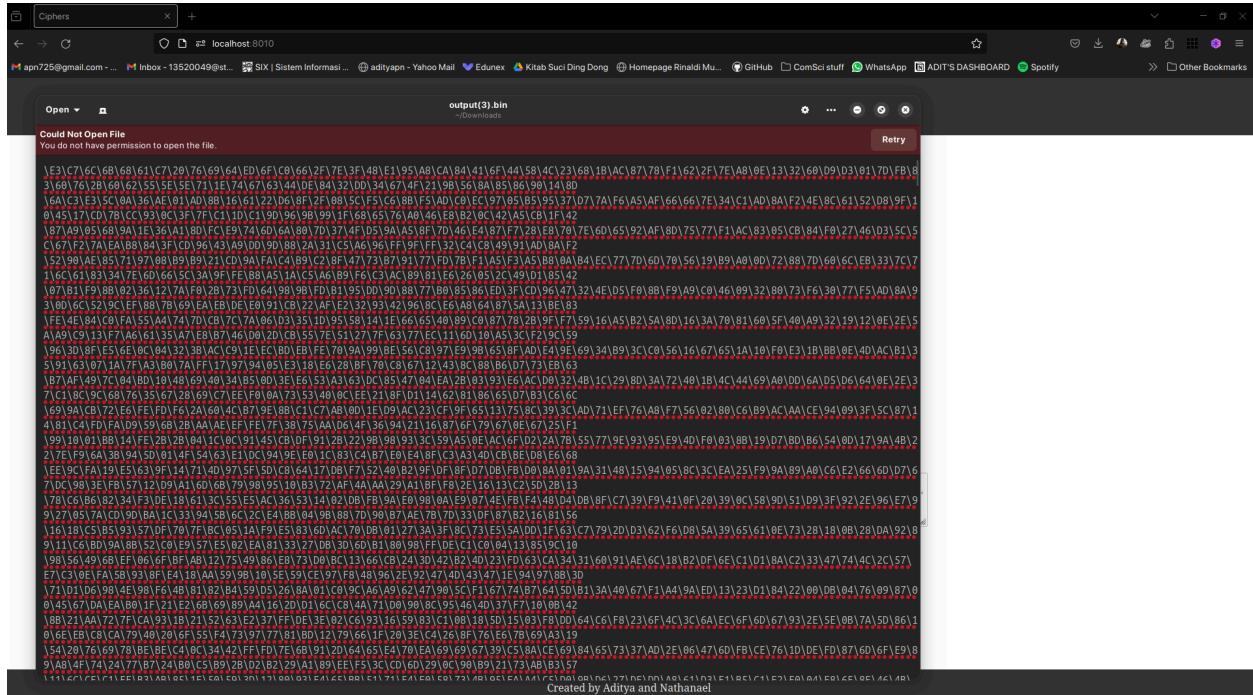
Output text: [Large hex dump of the encrypted file]

Output bytes: [Large hex dump of the encrypted file]

Plaintext Base64

Download Download as binary

Created by Aditya and Nathanael



Created by Aditya and Nathanael

Hasil enkripsi file input.webm dengan kunci “melihat video” ke dalam bentuk plainteks dan binary

The screenshot shows a web browser window titled "Ciphers In Ruby". The application interface includes fields for "Input type" (set to "Text"), "Input text" (containing the string "melihat video"), "Cipher type" (set to "Super Encryption (Extended Vigenere Cipher and Transposition)"), and a "Key" field (also containing "melihat video"). Below these are "Encrypt" and "Decrypt" buttons. The "Output text" field is filled with a large amount of binary-like encrypted data, and the "Output bytes" field shows a list of byte values: [26, 69, 223, 163, 1, 0, 0, 0, 0, 0, 0, 16, 66, 130, 133, 119, 101, 98, 109, 0, 66, 135, 129, 2, 66, 133, 129, 2, 24, 83, 128, 103, 100, 0, 126, 119, 155, 116, 1, 89, 108, 8, 149, 77, 187, 1, 8, 6, 6, 6, 0, 1, 83, 171, 132, 21, 73, 169, 182, 83, 172, 136, 0, 0, 0, 0, 0, 0]. At the bottom are buttons for "Plaintext", "Base64", "Download", and "Download as binary". To the right of the browser window, a VLC media player window is open, displaying a video file named "output.webm". The video player interface shows playback controls and a progress bar indicating the video is at 00:00.

Created by Aditya and Nathanael

Hasil dekripsi file binary dengan kunci “melihat video” ke dalam bentuk plainteks dan webm

8. Enigma Cipher

e. Input/Output Plainteks

Ciphers In Ruby

Ciphers In Ruby

Input type:

Input text:
a line, but it blazed in his mind for the
next minute as if stamped there with fiery
steel. "Time has fallen asleep in the
afternoon sunshine." He dropped the book.
Immediately, another fell into his arms."

Cipher type:

Key: bq cr di ej kw mt os px uz gh

Output text:

Output bytes:

Created by Aditya and Nathanael

Hasil enkripsi plainteks "*Books bombarded his shoulder, his arms, his upturned face. A book lit, almost obediently, like a white pigeon, in his hands, wings fluttering. In the dim, wavering light, a page hung open and it was like a snowy feather, the words delicately painted thereon. In all the rush and fervor, Montage had only an instant to read a line, but it blazed in his mind for the next minute as if stamped there with fiery steel. "Time has fallen asleep in the afternoon sunshine." He dropped the book. Immediately, another fell into his arms.*" dengan kunci "bq cr di ej kw mt os px uz gh" dalam plainteks dan base64. Posisi awal rotor merupakan hasil seeded random dengan penjumlahan indeks ($a = 0, b = 1, \dots$) kunci

sebagai seed (Kunci merupakan masukan plugboard). Misalkan dengan contoh kunci di atas, hasil penjumlahan indeks adalah 251, dan hasil angka acak posisi awal rotor adalah 25, 11, 1. Kode internal sebagai berikut:

```
key = "bqcrdiejkwmtojspxuzgh"  
  
# Using the plugboard key, get a seed value  
seed = key.chars.map { |c| c.ord - 'a'.ord }.sum  
puts seed  
srand(seed)  
  
for i in 0..2 do  
  puts rand(26)  
end
```

STDIN

Input for

Output:

251

25

11

1

Ciphers In Ruby

Input type:	Text
Input text:	prurctqwdmthfnbxhqrvtklavhfqwedvikxwbizdl drddgsvqiwosluvugkqpfvzjeqvnjk1fzungzgaectz ymnopciotkxgolypkbayjdqkoldqimmrkvbajjtbxz gkrxmciuvwsasfktyxugadpeswzqskmbmmmvgdhtq vbaeekzfpbwuzmzhrcxkpyttjvttzjbyrrvignvzlif
Cipher type:	Enigma
Key:	bq cr di ej kw mt os px uz gh
Encrypt	Decrypt
Output text:	booksbombardedhisshoulderhisarmshisupturnedfaceabooklitalmos tobedientlylikeawhitepigeoninhishandswingslutteringinthedim wavinglightapagehungopenanditwaslikeasnowyfeatherthewordsd elicatelypaintedtherewereonalltherushandfervormontagehadonly instanttoareadolinebutblazedinhismindfortheminuteasifst
Output bytes:	[98, 111, 111, 107, 115, 98, 111, 109, 98, 97, 114, 100, 101, 100, 104, 105, 115, 115, 104, 111, 117, 108, 100, 101, 114, 104, 105, 115, 97, 114, 109, 115, 104, 105, 115, 117, 112, 116, 117, 114, 110, 101, 100, 102, 97, 99, 101, 97, 98, 111, 111, 107, 108, 105, 116, 97, 108, 109, 111, 115, 116,
Plaintext	Base64
Download	Download as binary

Created by Aditya and Nathanael

Hasil dekripsi plainteks

“prurctqwdmthfnbxhqrvtklavhfyqwedvikxwbizldrrddgsqvqiwosluvugkqpfzvje qvnjklfzungzgaecztymzoppciotkxgolypkbayjdqkoldqimmrkvabajtbxzgkrxmcin vuwsasfktytxugadpeswzqskmbmmnvvgdhtqvbaeekzfpbwuzmzhrcxkpyttjvttzj byrrvignvzlifshkuaxyeaxmyjoufopfxhdkrqemceghocaugjjzssguqaqgrsqnidpf egziyhcpawbkbggssrmxddhraktkyvsekyfoyhjkdsbastuzkxtdqqqwzfjfwnwdzk pkcrococpjsnimjpkybqtflifoevsyiixicgeqlhkuznagxfnxgjrkuaiobznnkwsainx ydmdzu” dengan kunci “bq cr di ej kw mt os px uz gh”

f. Input/Output File Teks “input.txt”

Ciphers In Ruby

Input type:

Input text:

Cipher type:

Key:

Output text:

Output bytes:

Created by Aditya and Nathanael

```
input.txt x ...
CiphersInRuby > example_input > input.txt
1   Kriptografi asik sekali 99 juta kali bro!!!!
2   |
```

```
input.txt    output.txt U x ...
CiphersInRuby > example_input > output.txt
1   lnpkbxwdetjzbemcvnofqnevcxcobyze
```

Hasil enkripsi *file* dengan kunci “bumi” dalam bentuk file “output.txt”

Ciphers In Ruby

Input type:

Input text:

Cipher type:

Key:

Output text:

Output bytes:

Created by Aditya and Nathanael

Hasil dekripsi file “output.txt” dalam bentuk plainteks dengan kunci “bumi”.

Link Github

<https://github.com/nart4hire/CiphersInRuby>

Link Live Demo

<https://ciphers.nathancs.dev>

(Situs baru muncul saat repository sudah bisa publik)

Checklist

No	Spek	Berhasil (✓)	Kurang Berhasil (✗)	Keterangan
1.	Vigenere Cipher standard (26 huruf alfabet)	✓		
2.	Varian Vigenere Cipher standard (26 huruf alfabet): Auto-Key Vigenere Cipher	✓		
3.	Extended Vigenere Cipher (256 karakter ASCII)		✓	Dalam melakukan dekripsi plainteks, Ruby akan melakukan konversi karakter spesial berdasarkan encoding “UTF-8” sehingga kemungkin n representasi integer melebihi 255
4.	Playfair Cipher (26 huruf alfabet)	✓		
5.	Affine Cipher (26 huruf alfabet)	✓		

6.	Hill Cipher (26 huruf alfabet)	✓		
7.	Super enkripsi	✓		
8.	(Bonus) Enigma cipher	✓		
9.	(Bonus) Bahasa Ruby	✓		