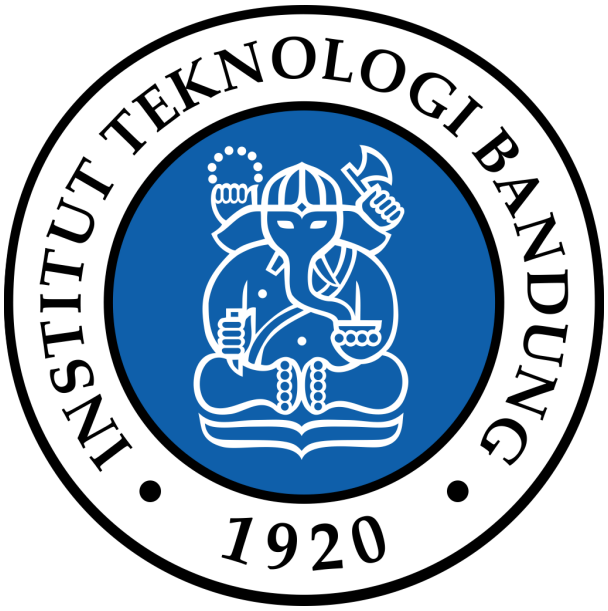
Laporan Tugas 1 IF4020 Kriptografi
Implementasi Algoritma Cipher

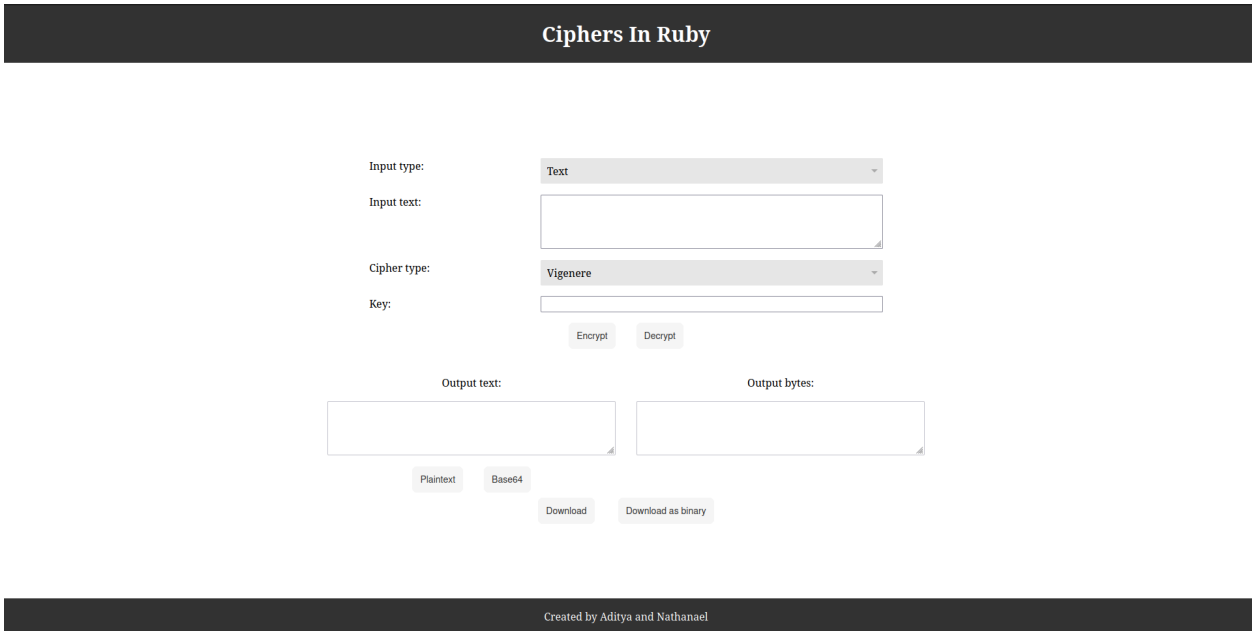


Oleh:
Aditya Prawira Nugroho - 13520049
Nathanael Santoso - 13520129

TEKNIK INFORMATIKA
SEKOLAH TEKNIK ELEKTRO DAN INFORMATIKA
INSTITUT TEKNOLOGI BANDUNG
2024

Daftar Isi

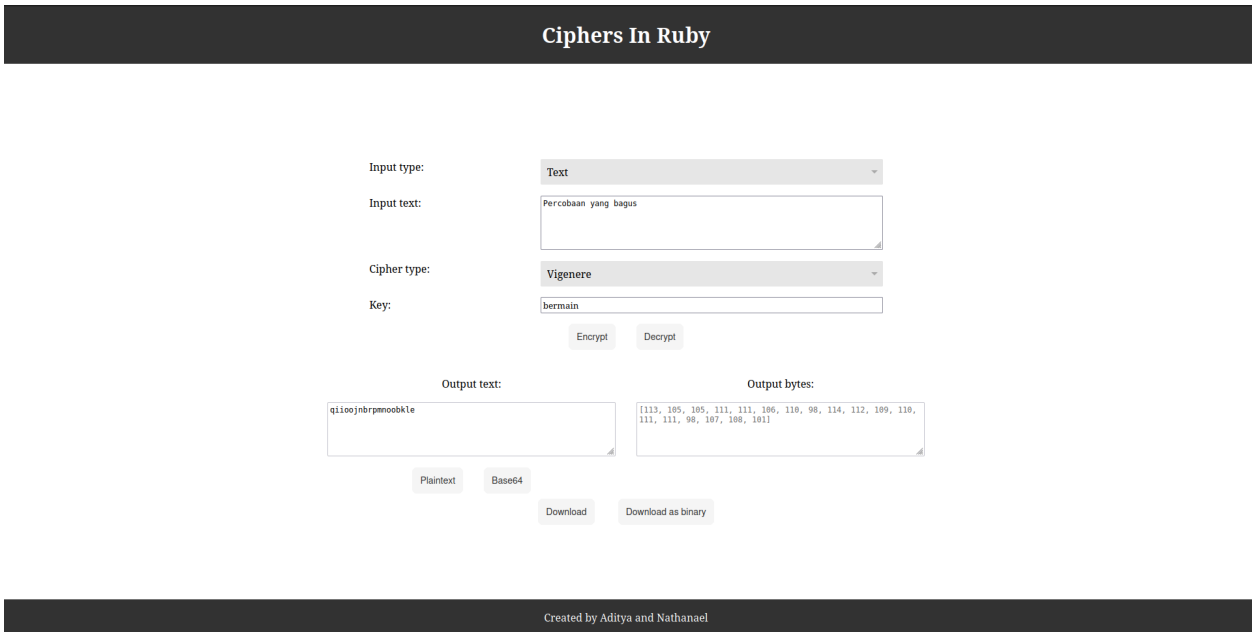
Tampilan Antarmuka Program

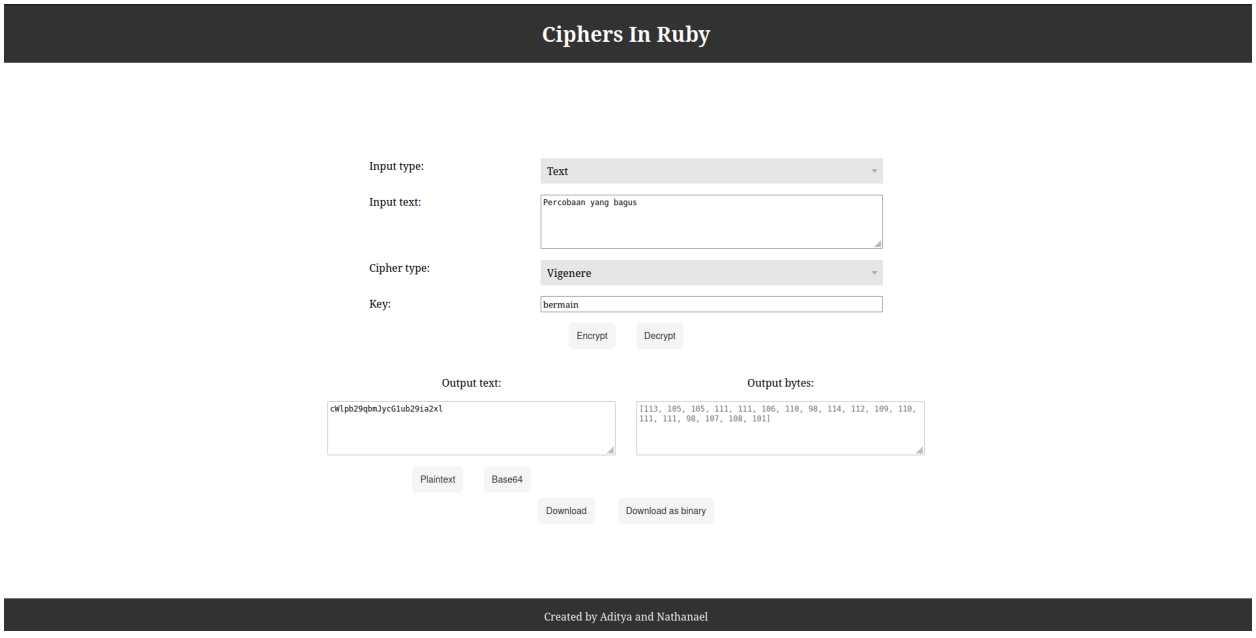


Contoh Plainteks dan Cipherteks

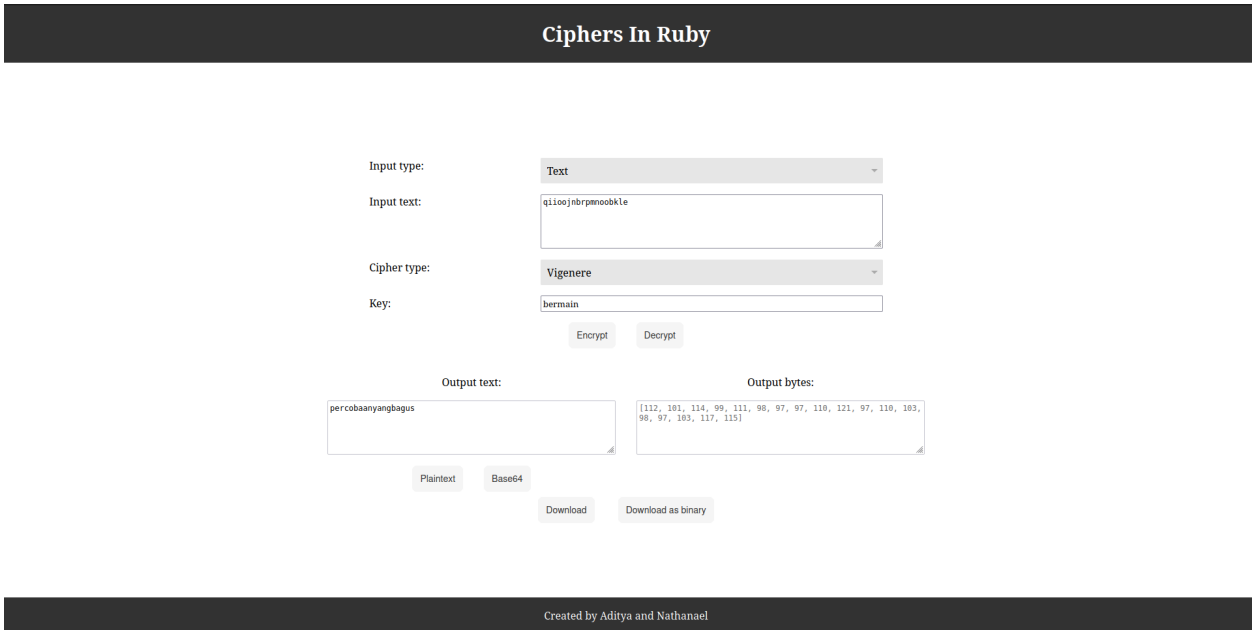
1. Vigenere Cipher Standard

a. Input/Output Plainteks



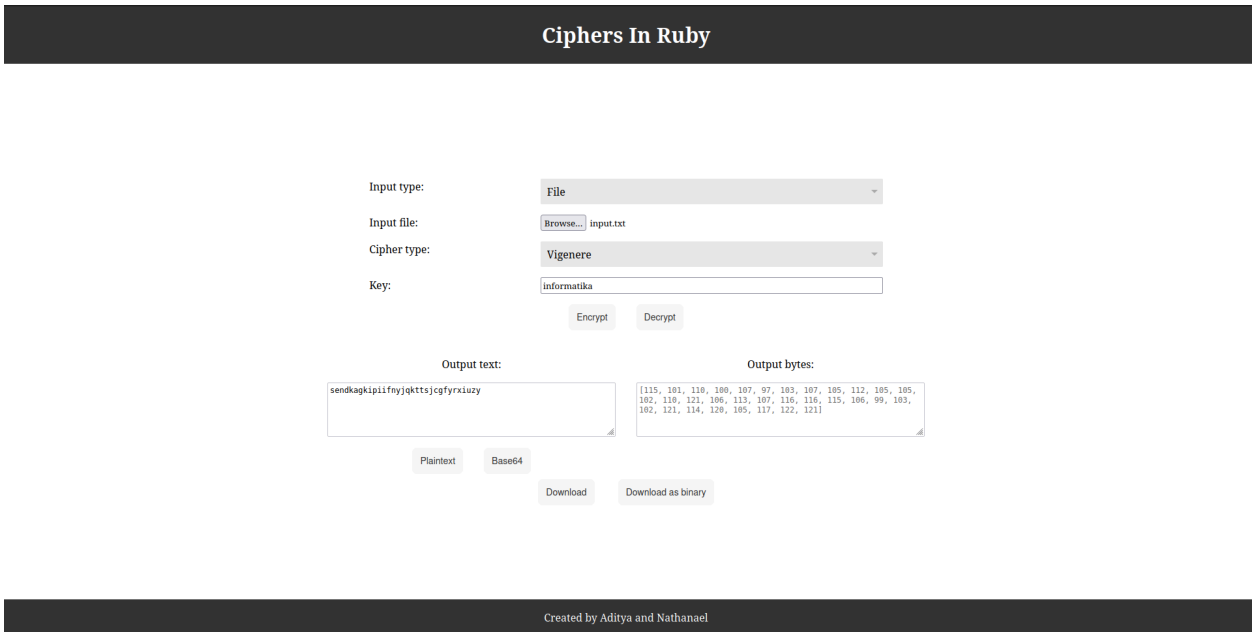


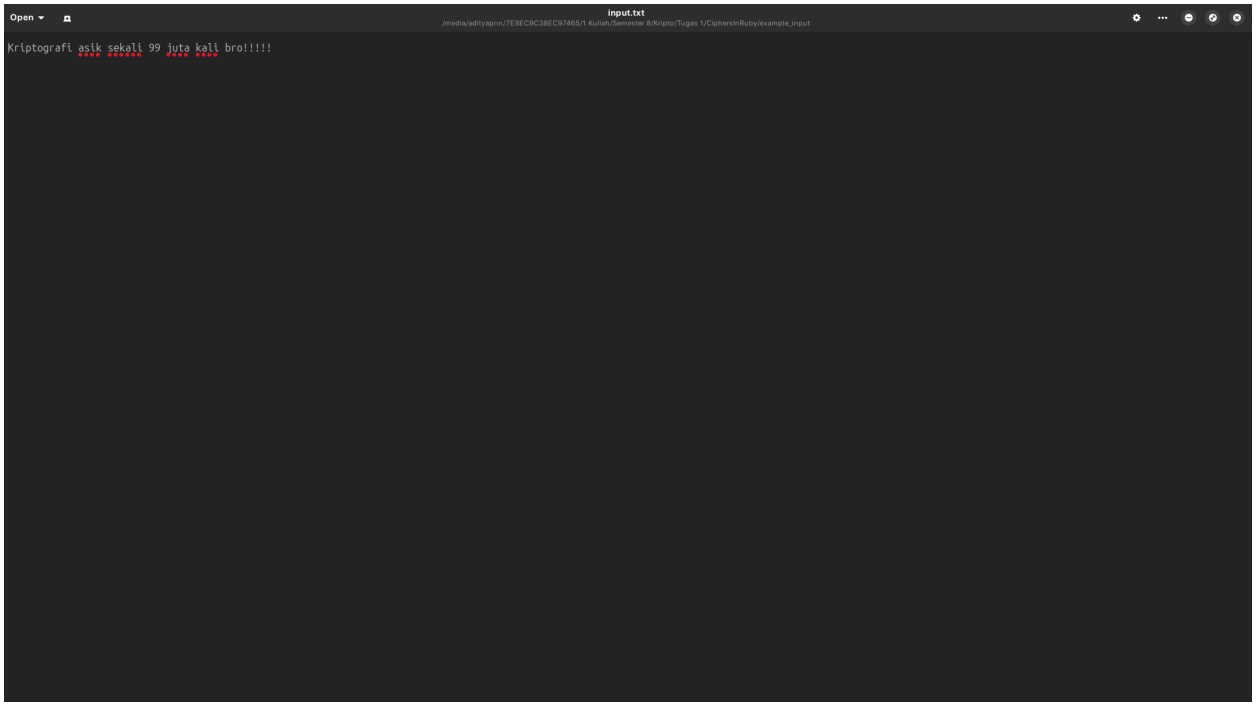
Enkripsi plainteks “Percobaan yang bagus” dengan kunci “bermain” dengan bentuk output plainteks dan base64



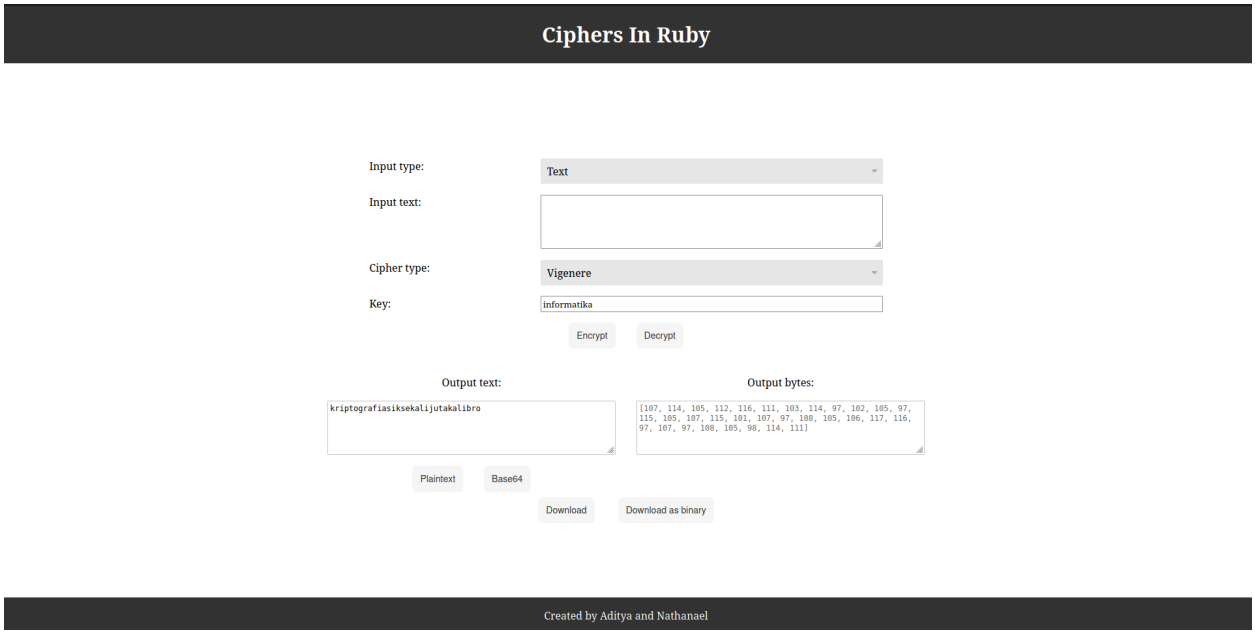
Dekripsi dari cipherteks “qiioojnbrpmnoobkle” dengan kunci “bermain”

b. Input/Output File Teks “input.txt”





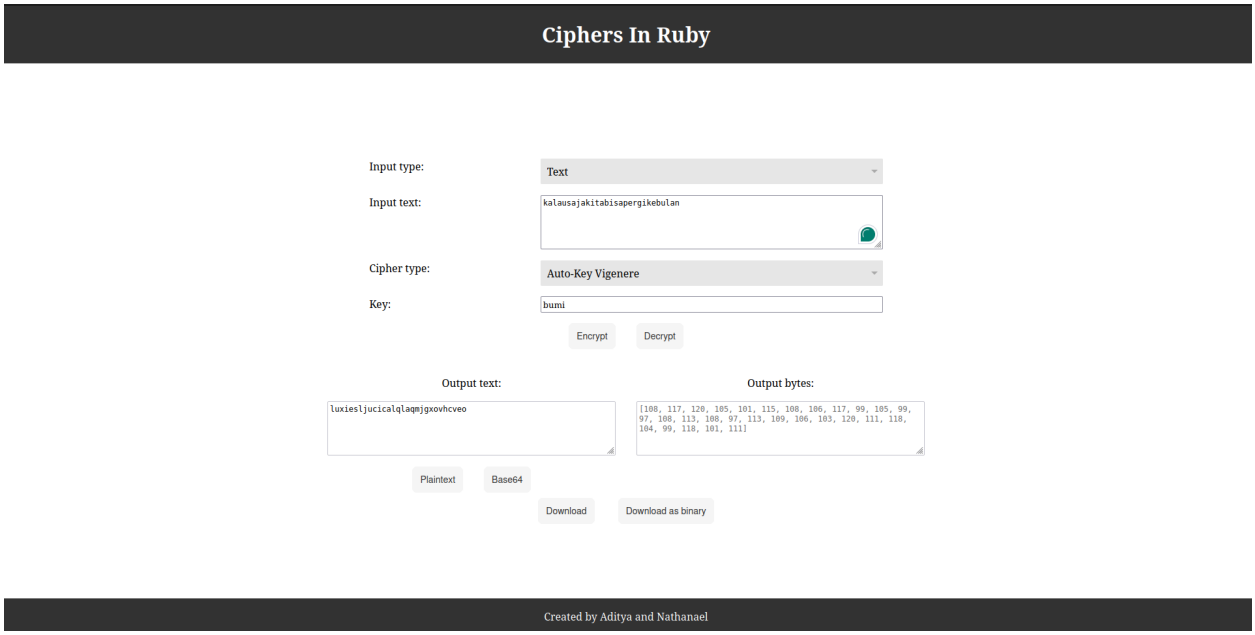
Hasil enkripsi isi dari file “input.txt” dalam bentuk plainteks dan file yang diunduh menjadi “output”.txt.

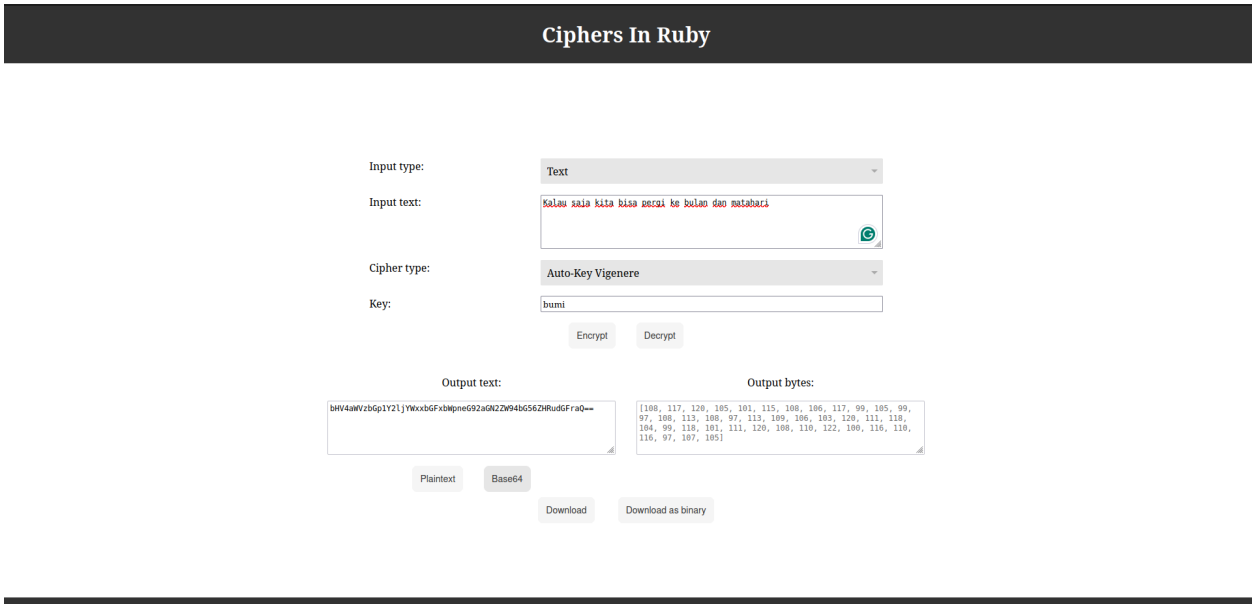


Hasil dekripsi file “output.txt” menjadi plainteks “kriptografiasiksekalijutakalibro” yang menghilangkan karakter spesial dan angka.

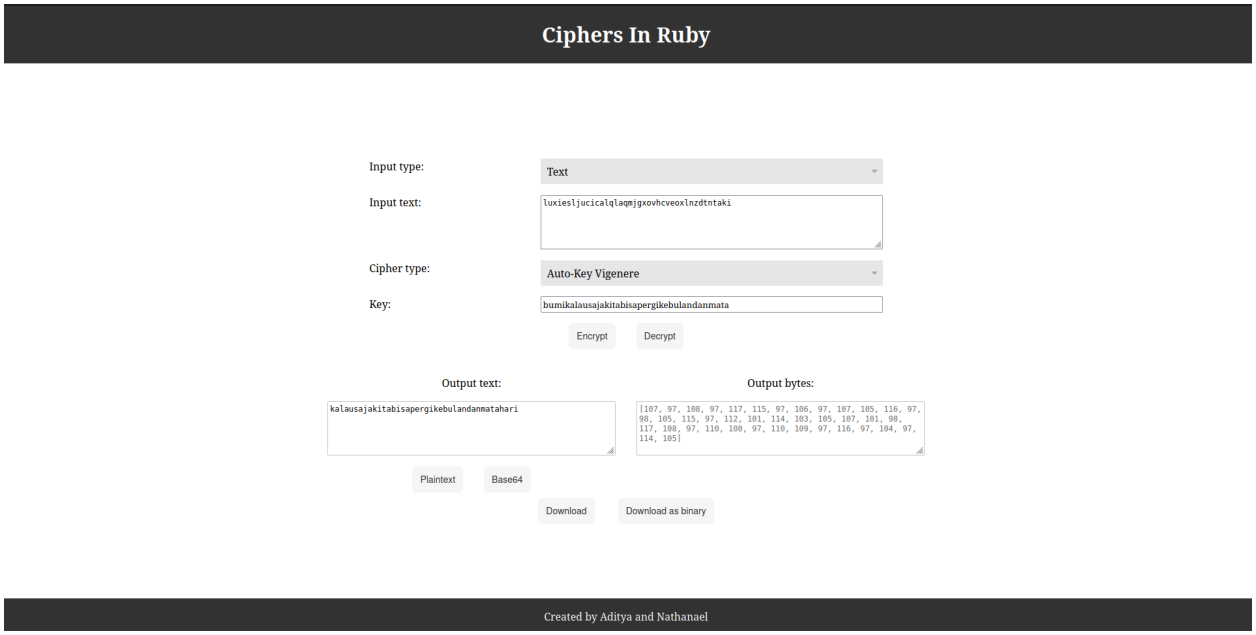
2. *Auto-Key* Vigenere Cipher

a. Input/Output Plainteks



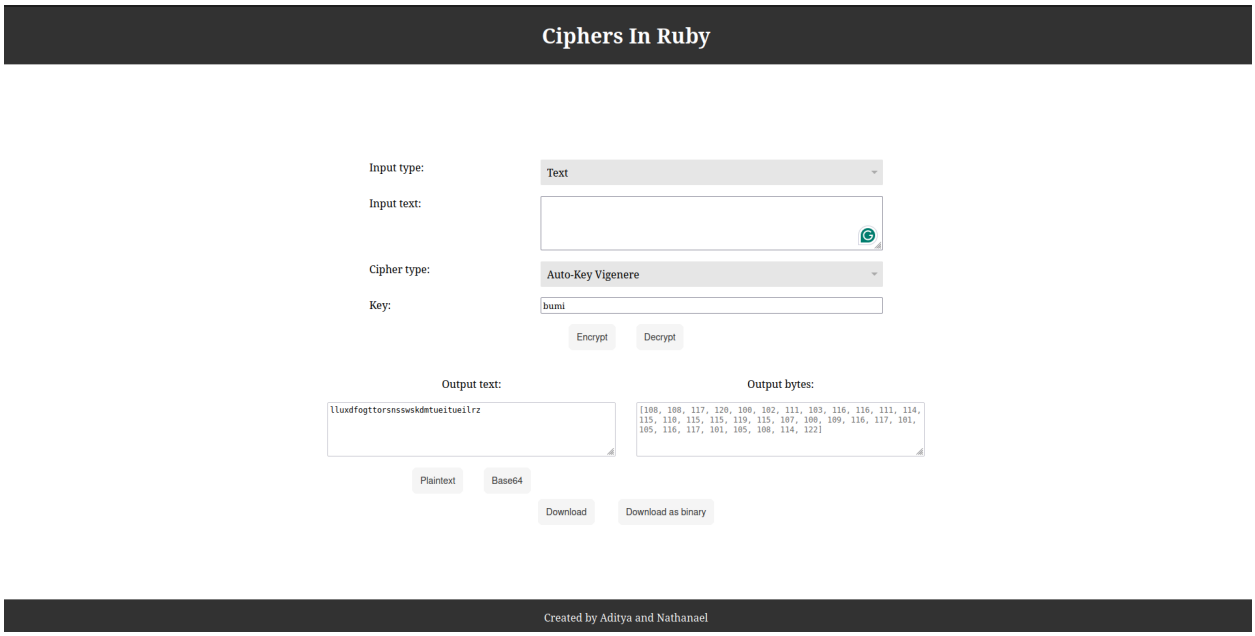


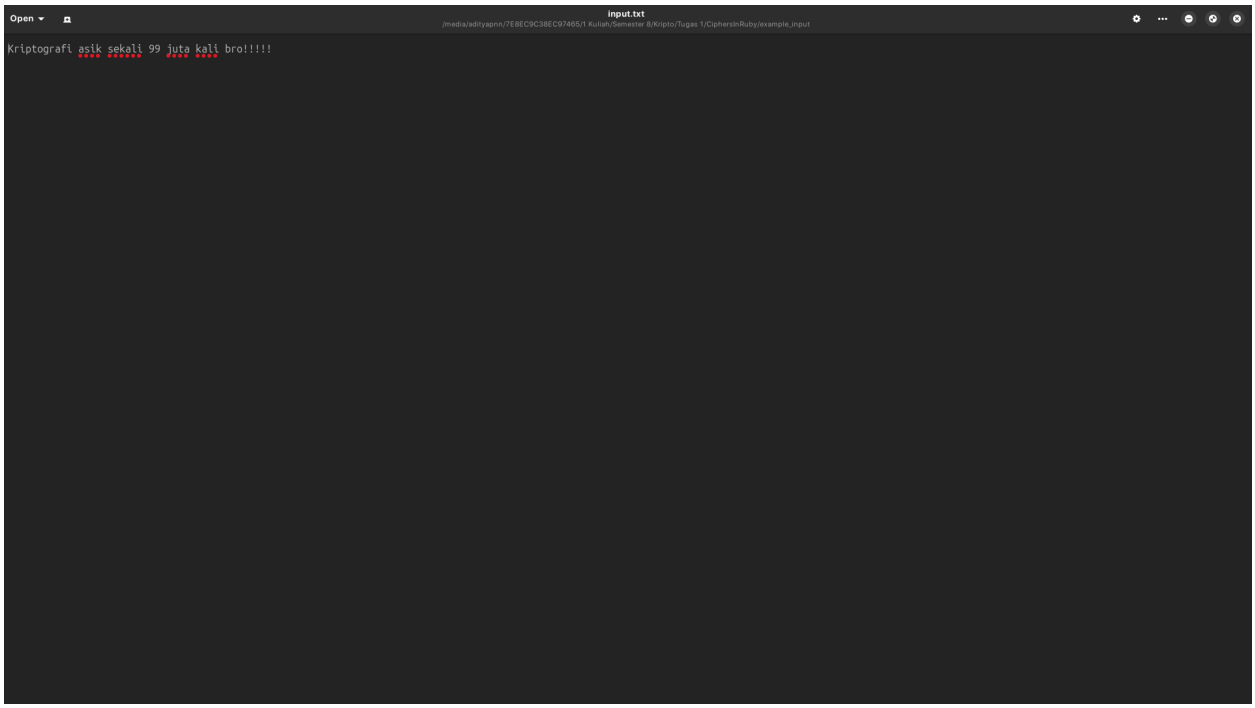
Hasil enkripsi plainteks “Kalau saja kita bisa pergi ke bulan dan matahari” dengan kunci “bumi” dalam plainteks dan base64

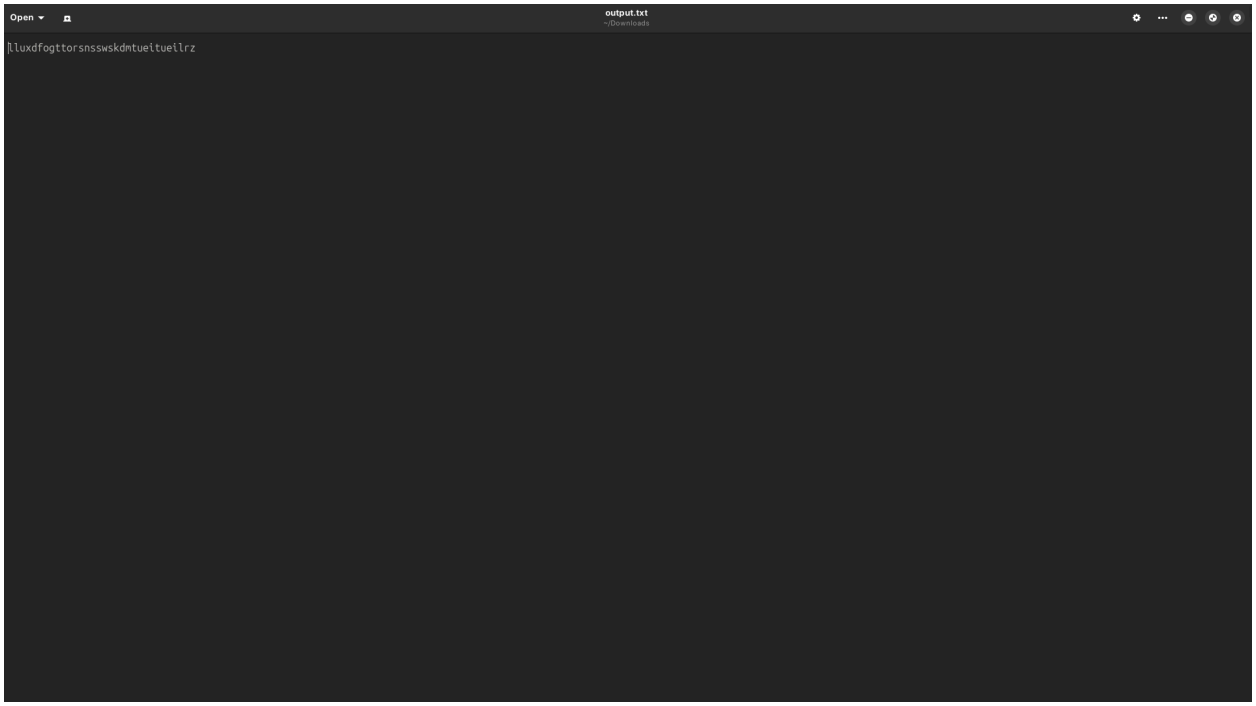


Hasil dekripsi plainteks “luxiesljucicalqlaqmjgxovhcveoxlnzdtntaki” dengan kunci “bumikalausajakitabisapergikebulandanmata”

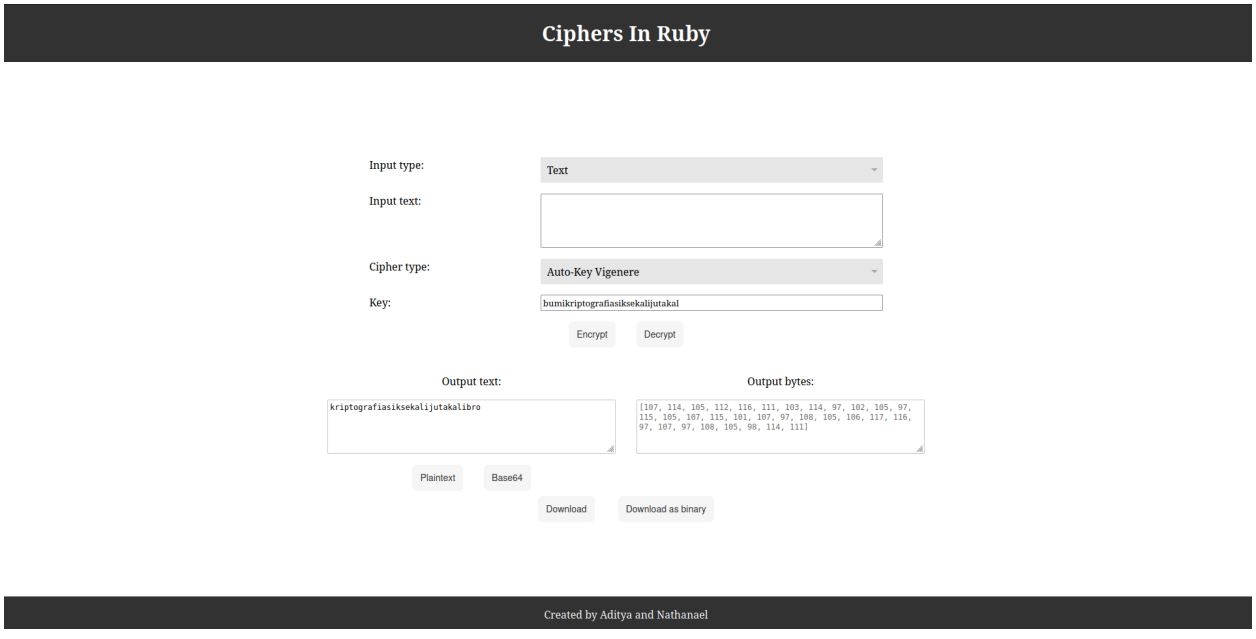
b. Input/Output File Teks “input.txt”







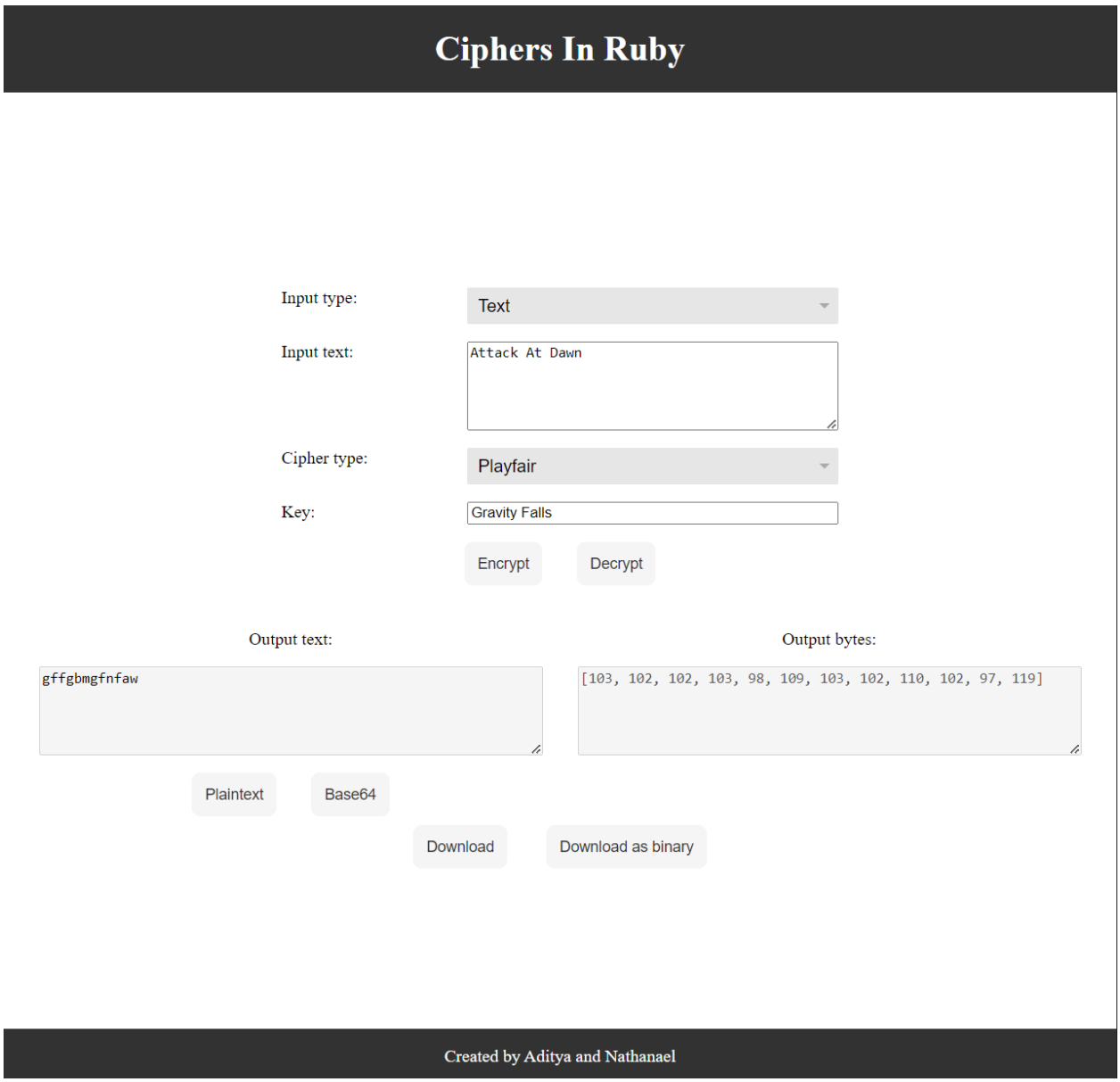
Hasil enkripsi *file* dengan kunci “bumi” dalam bentuk file “output.txt”

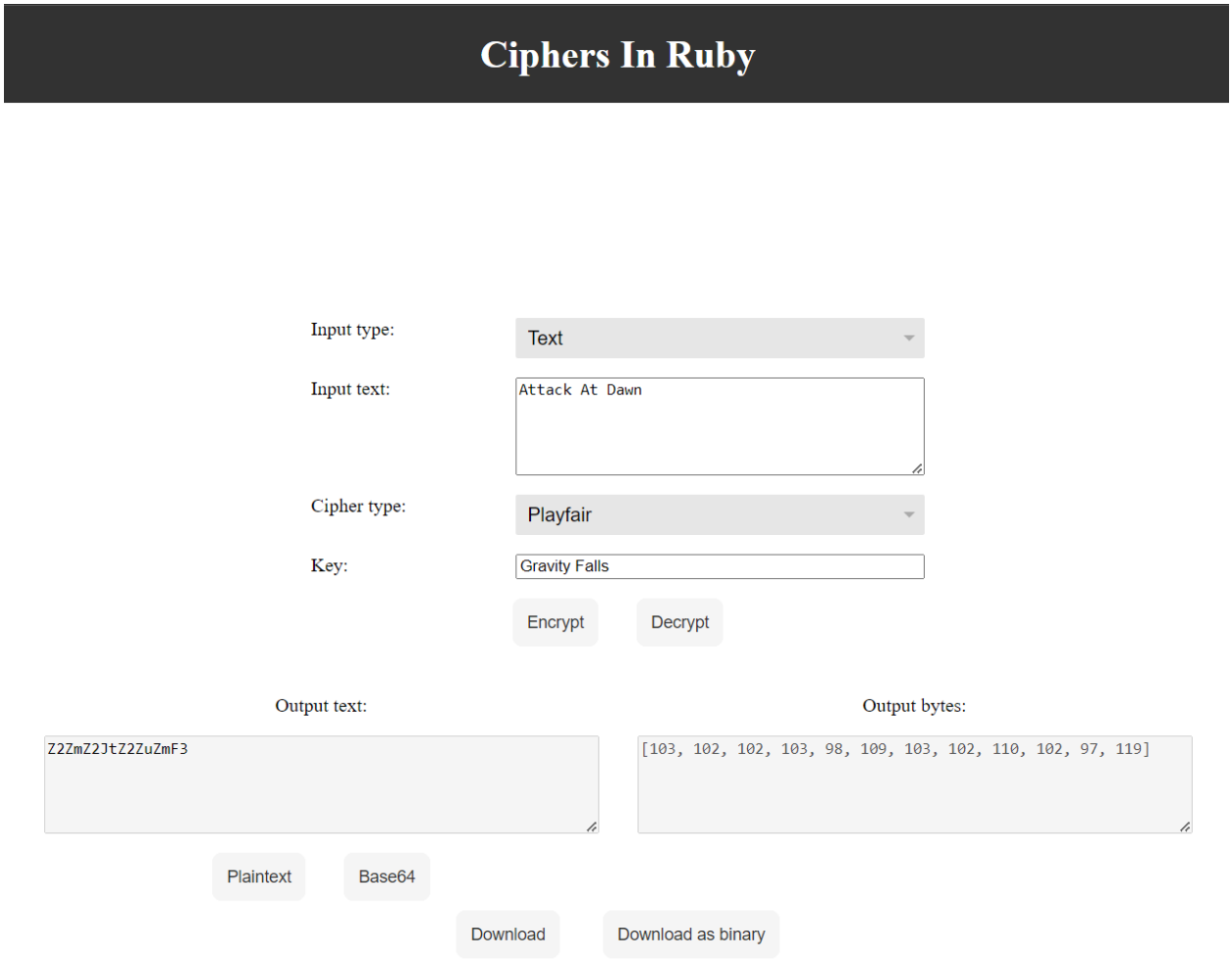


Hasil dekripsi *file* “output.txt” dalam bentuk plainteks dengan kunci “bumikriptografiasiksekalijutakal”

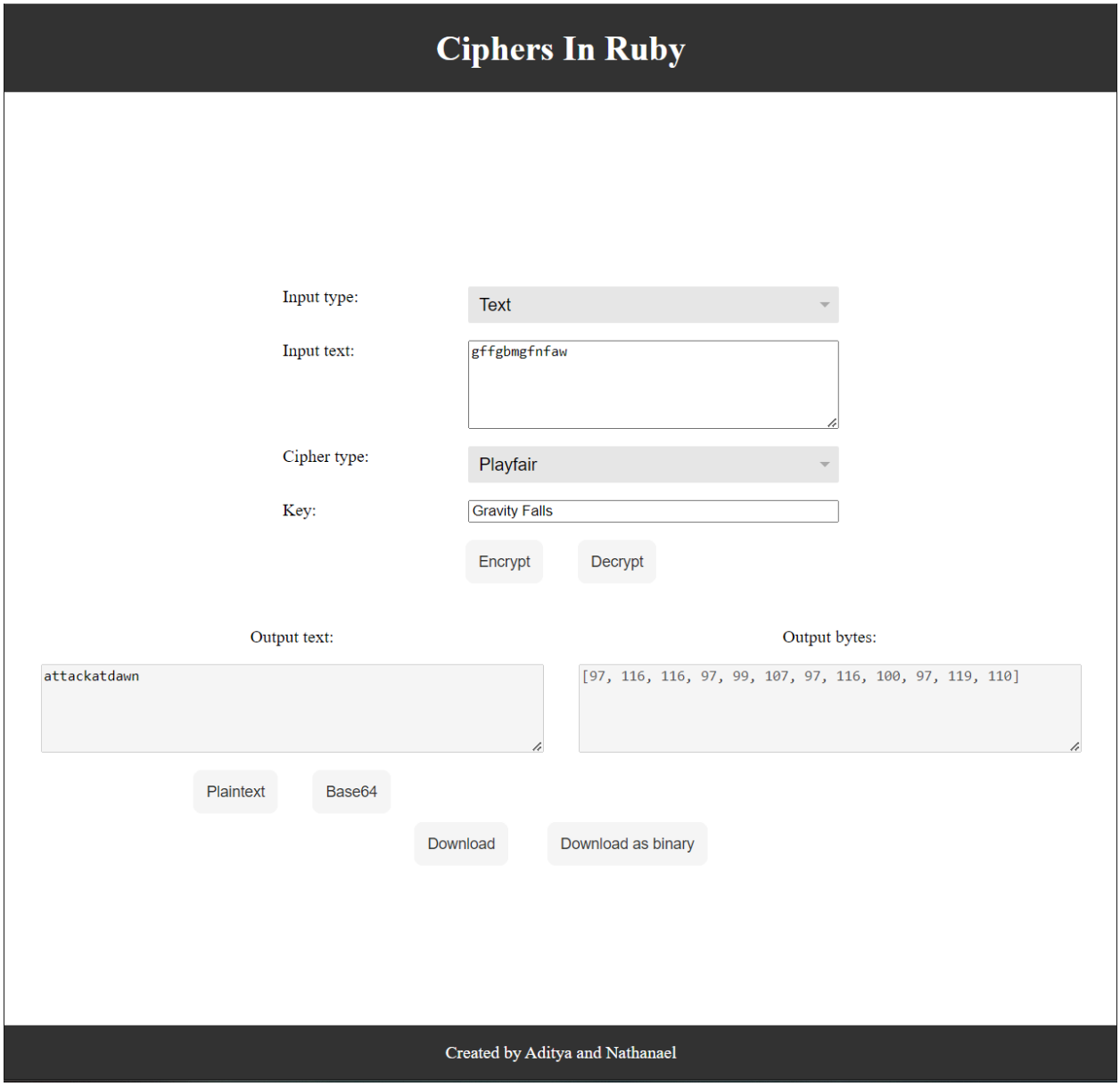
3. *Playfair Cipher*

a. Input/Output Plainteks



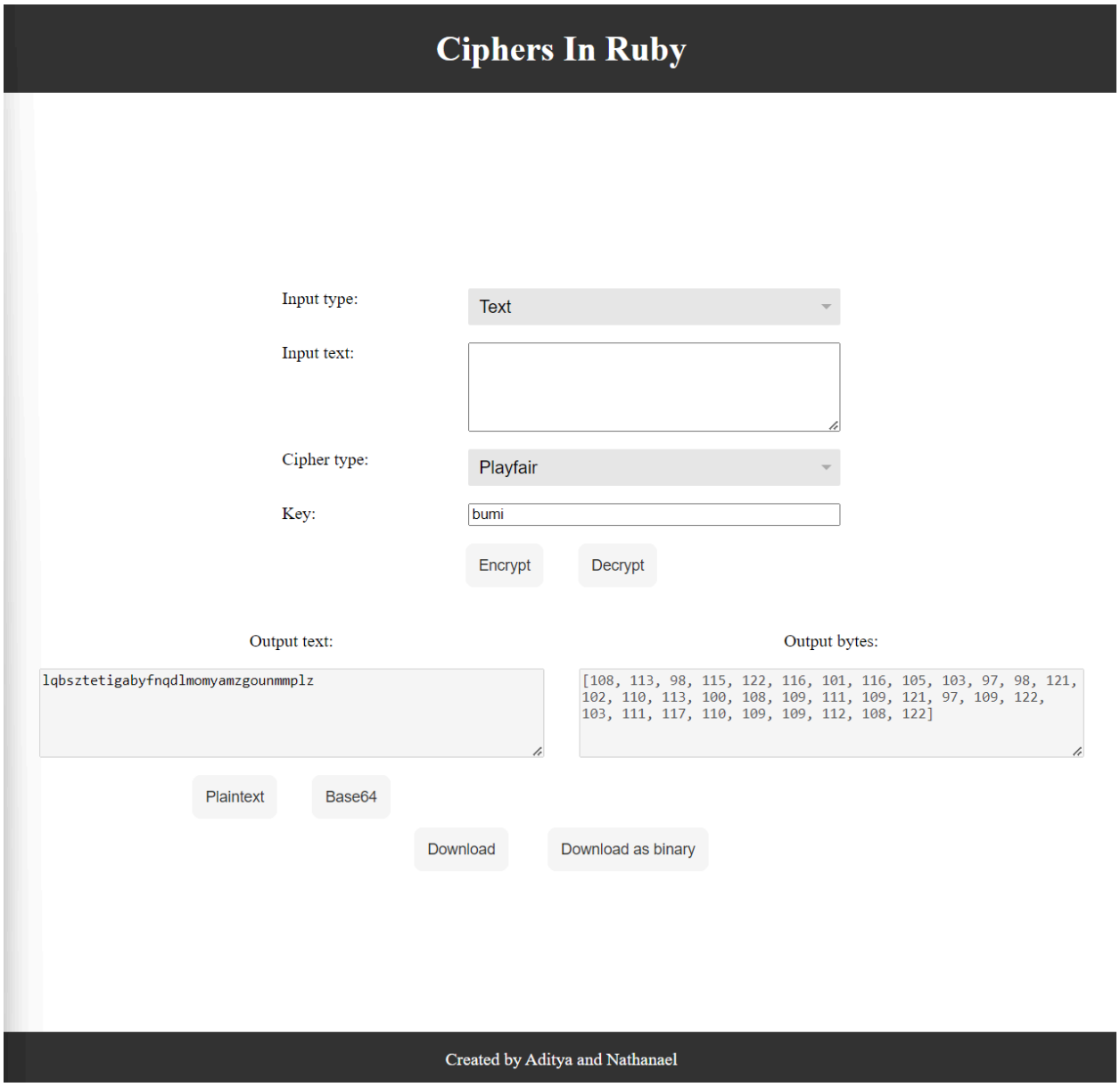


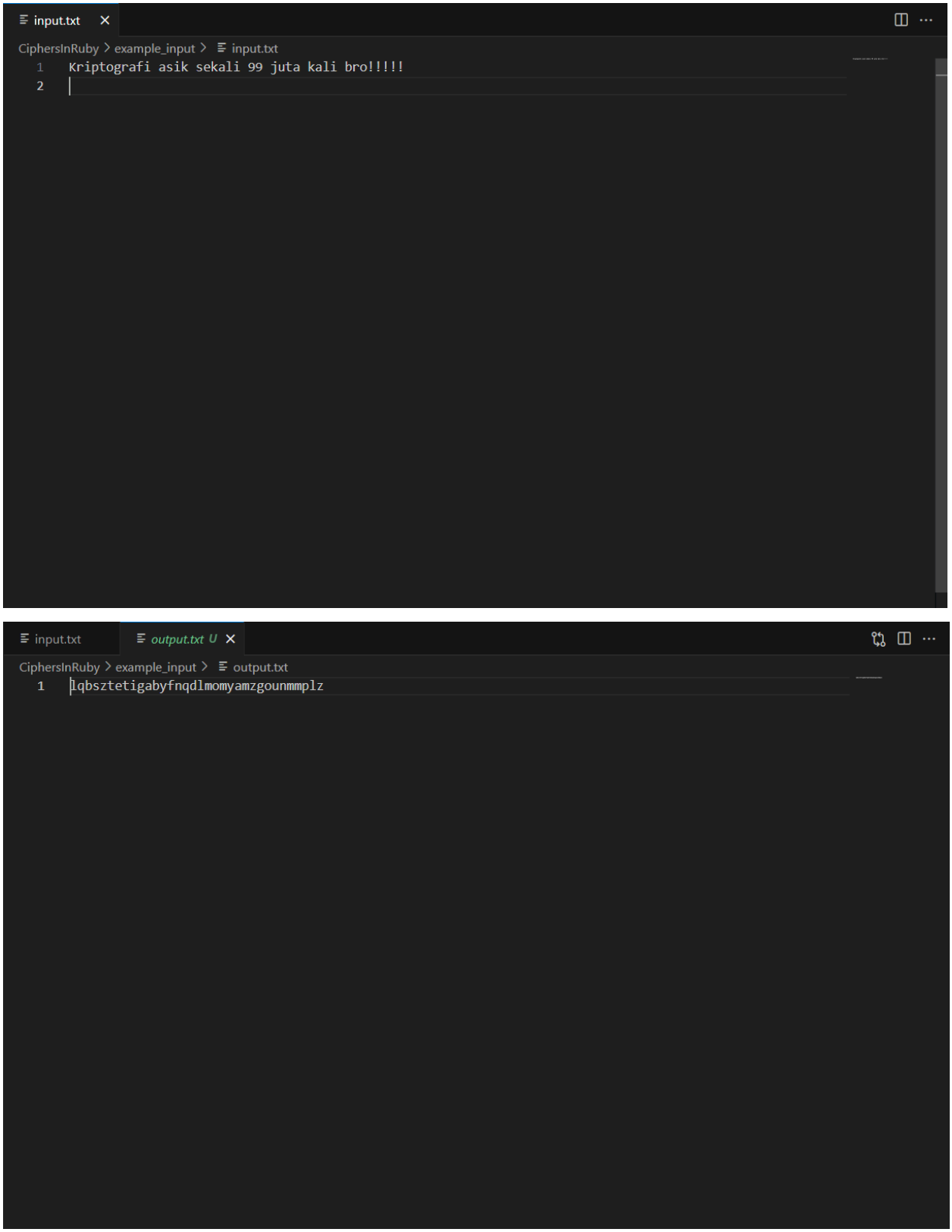
Hasil enkripsi plainteks “Attack At Dawn” dengan kunci “Gravity Falls” dalam plainteks dan base64



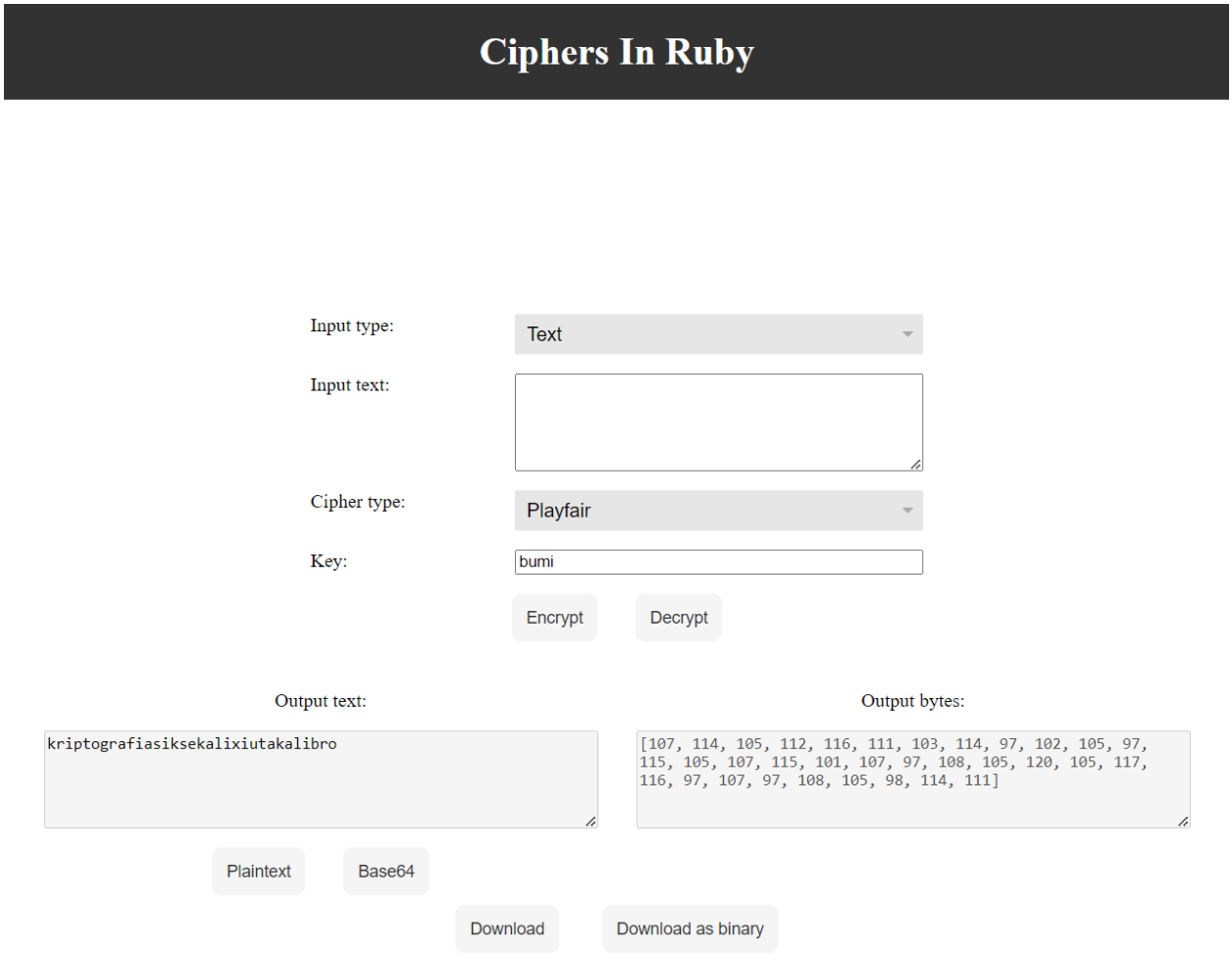
Hasil dekripsi plainteks “gffgbmgfnfaw” dengan kunci “Gravity Falls”

b. Input/Output File Teks “input.txt”





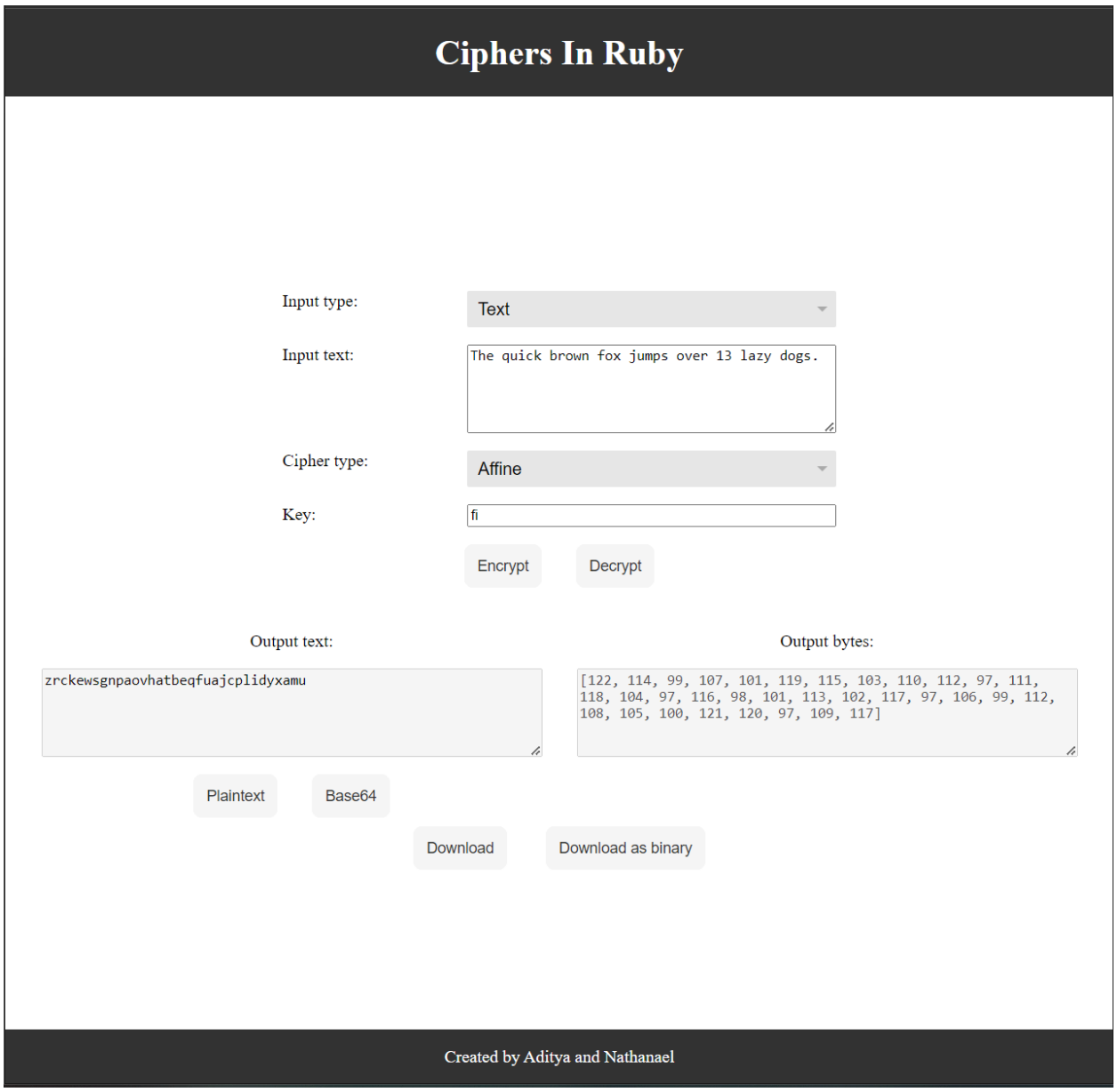
Hasil enkripsi *file* dengan kunci “bumi” dalam bentuk file “output.txt”

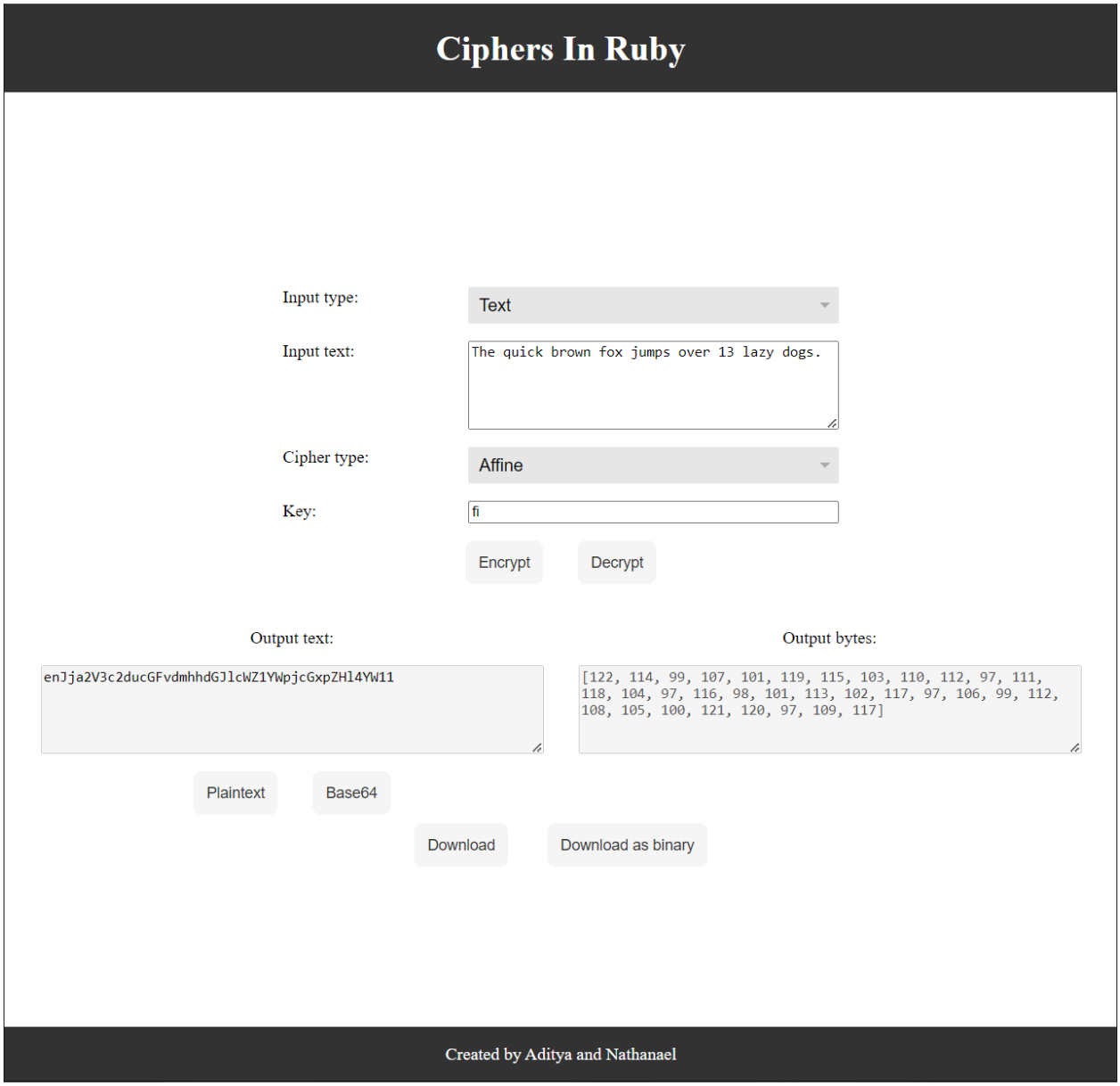


Hasil dekripsi *file* “output.txt” dalam bentuk plainteks dengan kunci “bumi”, diperhatikan karena algoritma Playfair naturnya *lossy* maka hasil menjadi “kriptografiasiksekalixiutakalibro” karena padding dan konversi ‘j’ ke ‘i’.

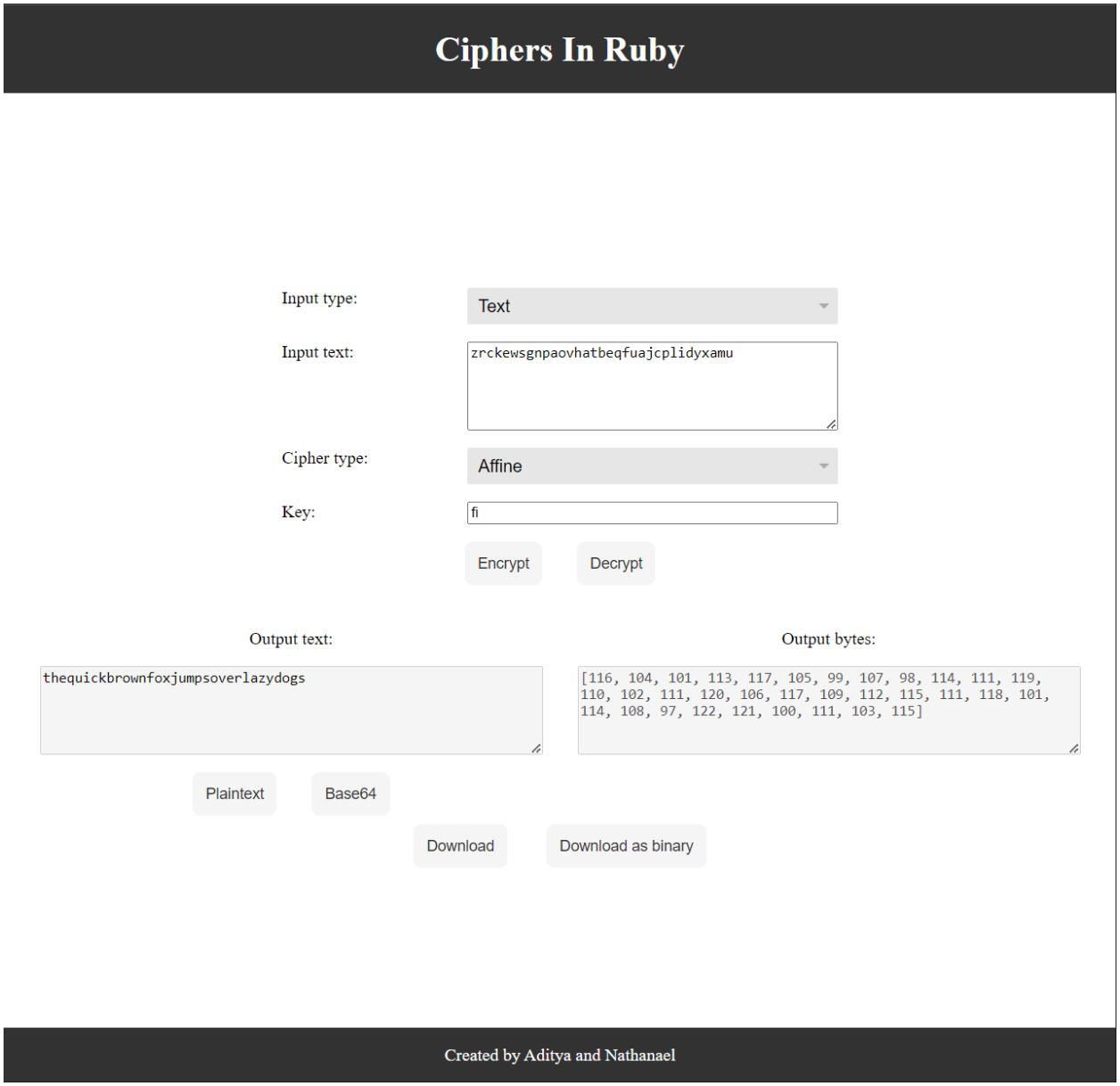
4. *Affine Cipher*

a. Input/Output Plainteks





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



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:

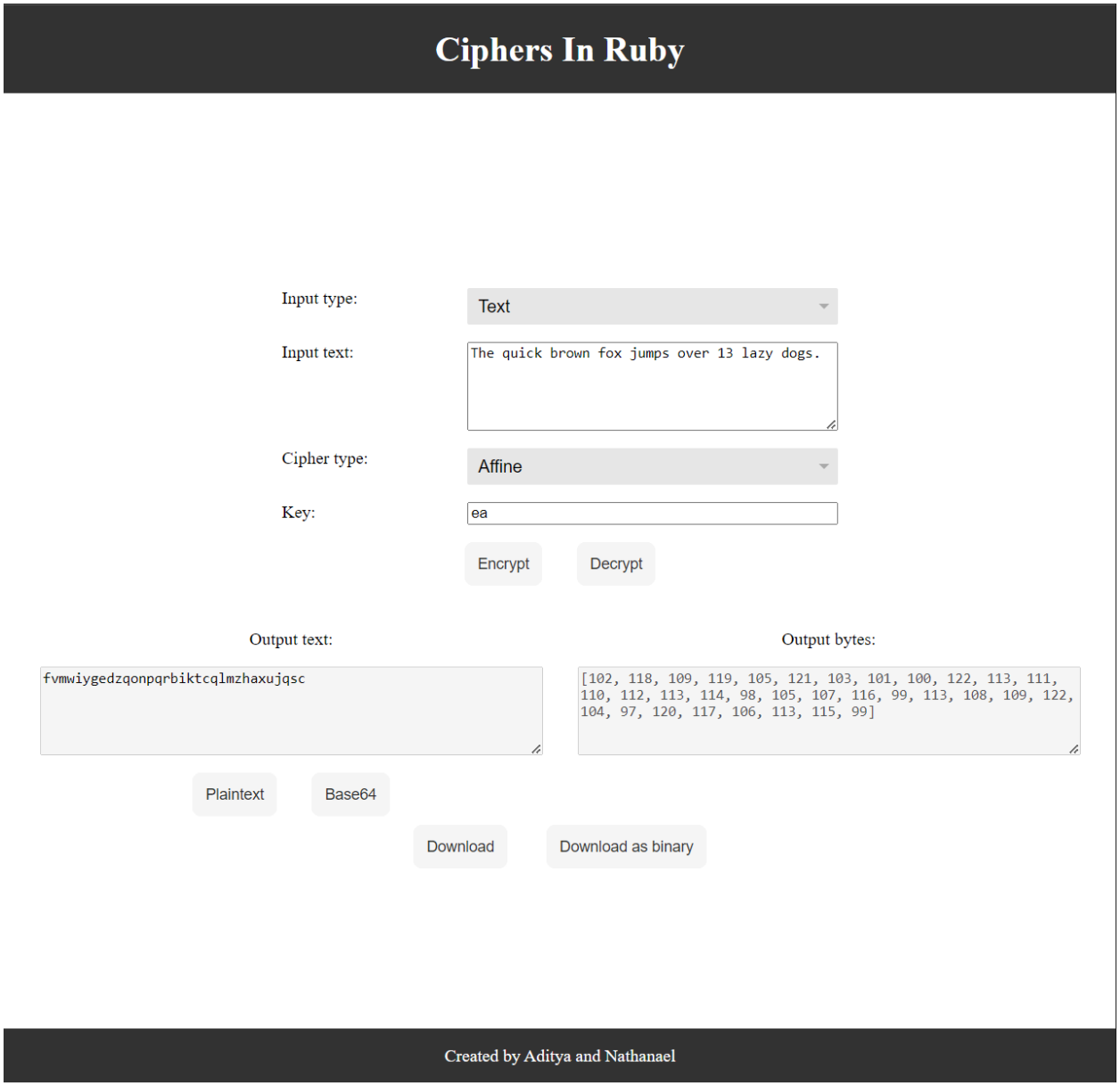
```
fvmwiygedzqonpqrbiktcqlmzhaxujqsc
```

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]
```

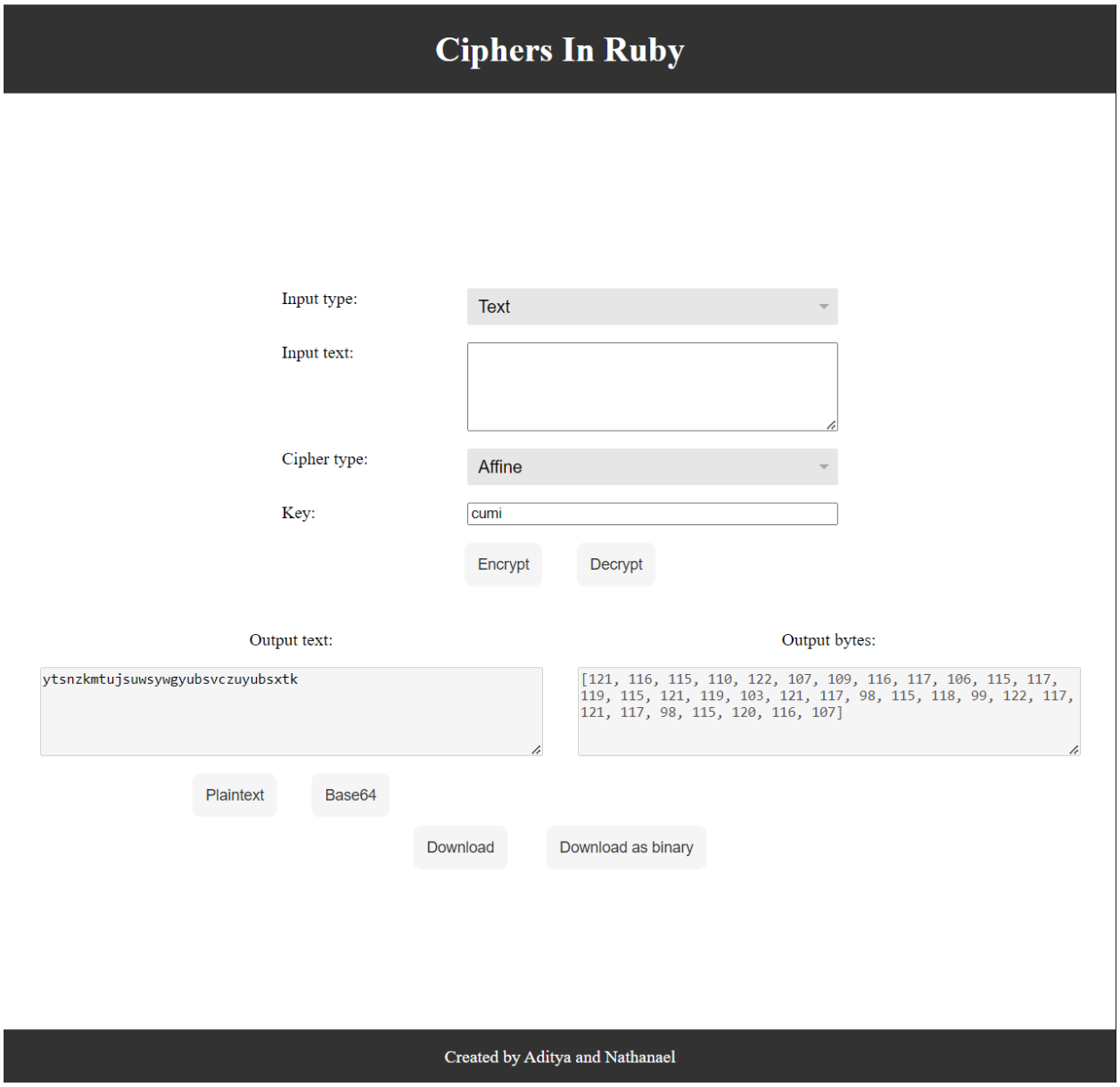
Plaintext Base64

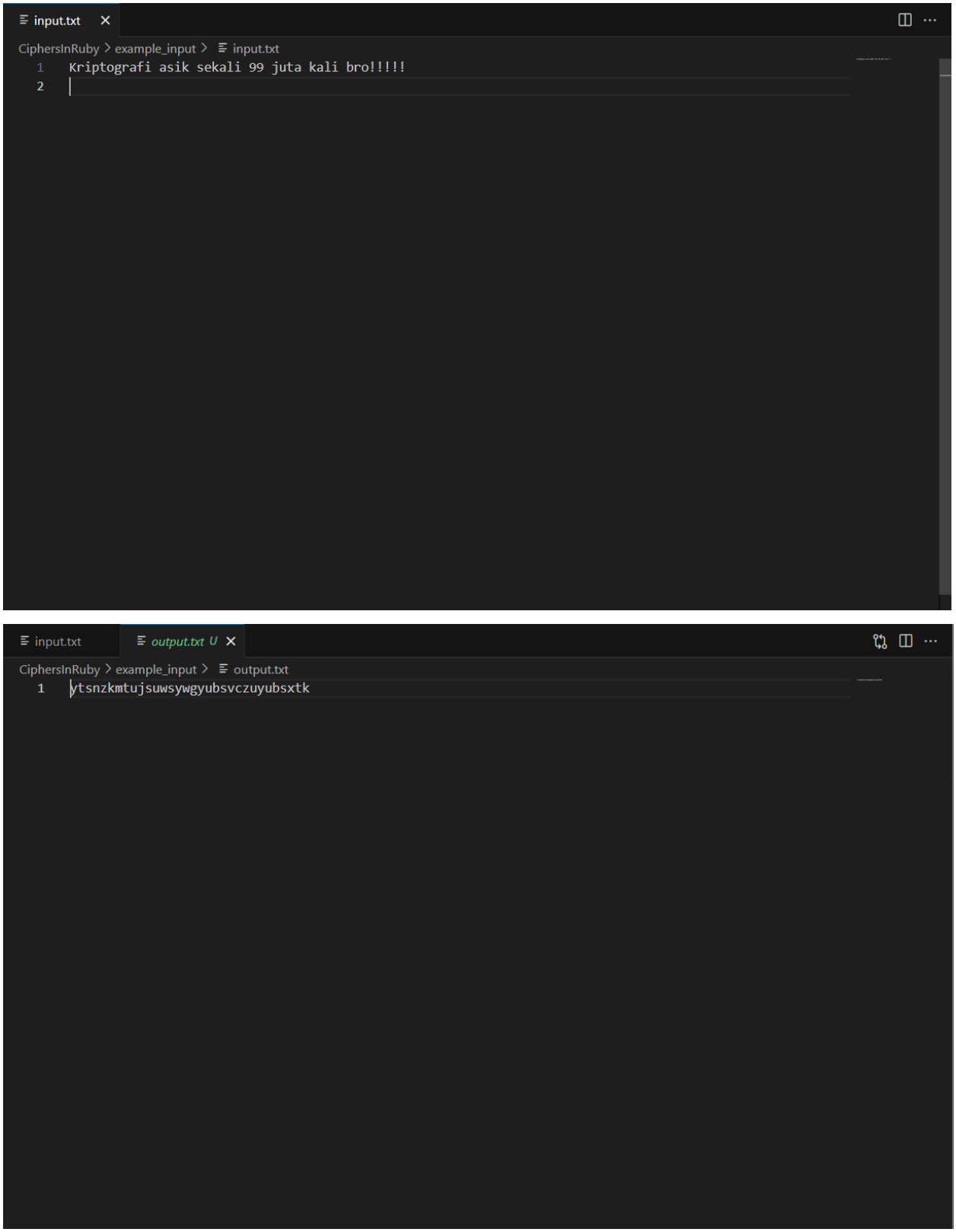
Download Download as binary



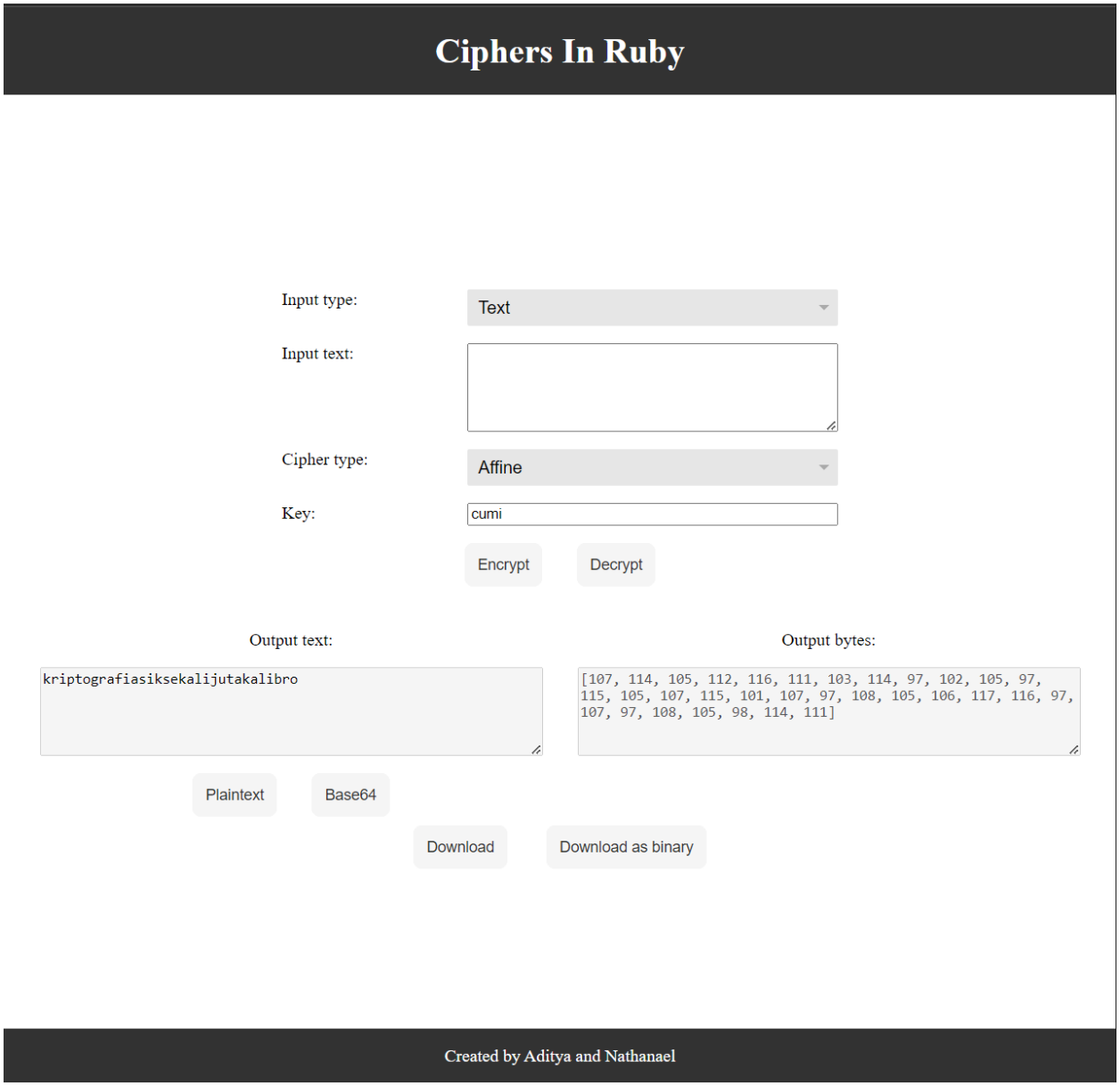
Hasil enkripsi plainteks “The quick brown fox jumps over 13 lazy dogs.” dengan kunci “ca” (a = 2, b = 0) dan “ea” atau (a = 4 b = 0). Karena kunci invalid, maka program otomatis menyetel kunci valid yaitu “da” atau (a = 3, b = 0)

b. Input/Output File Teks “input.txt”





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



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

5. *Hill Cipher*

c. Input/Output Plainteks

Ciphers In Ruby

Input type: Text

Input text:

```
thetruthisoutthere
```

Cipher type: Hill

Key: hillciphr

Encrypt Decrypt

Output text:

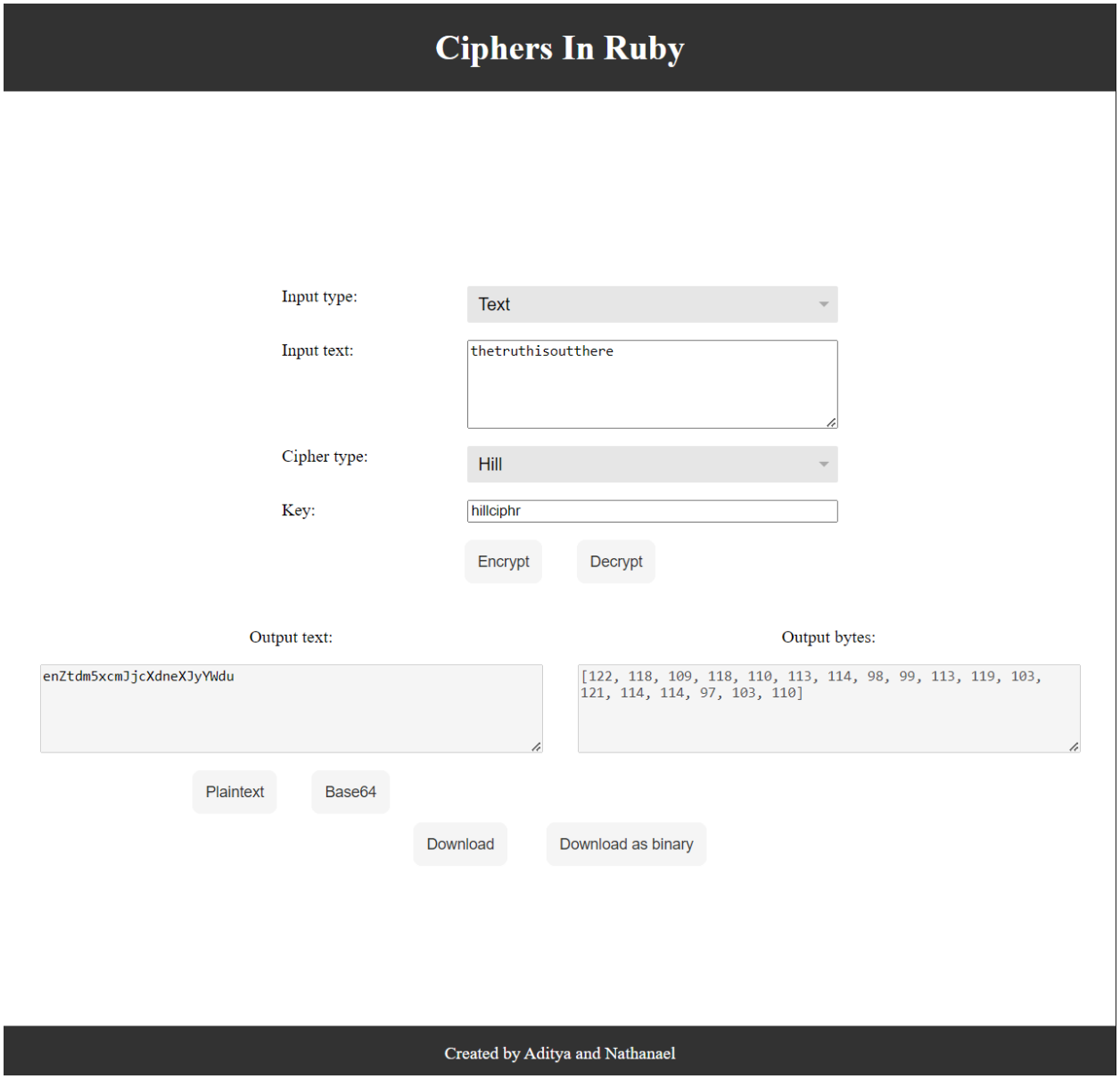
```
zvmvnqrbcqwgyrragn
```

Output bytes:

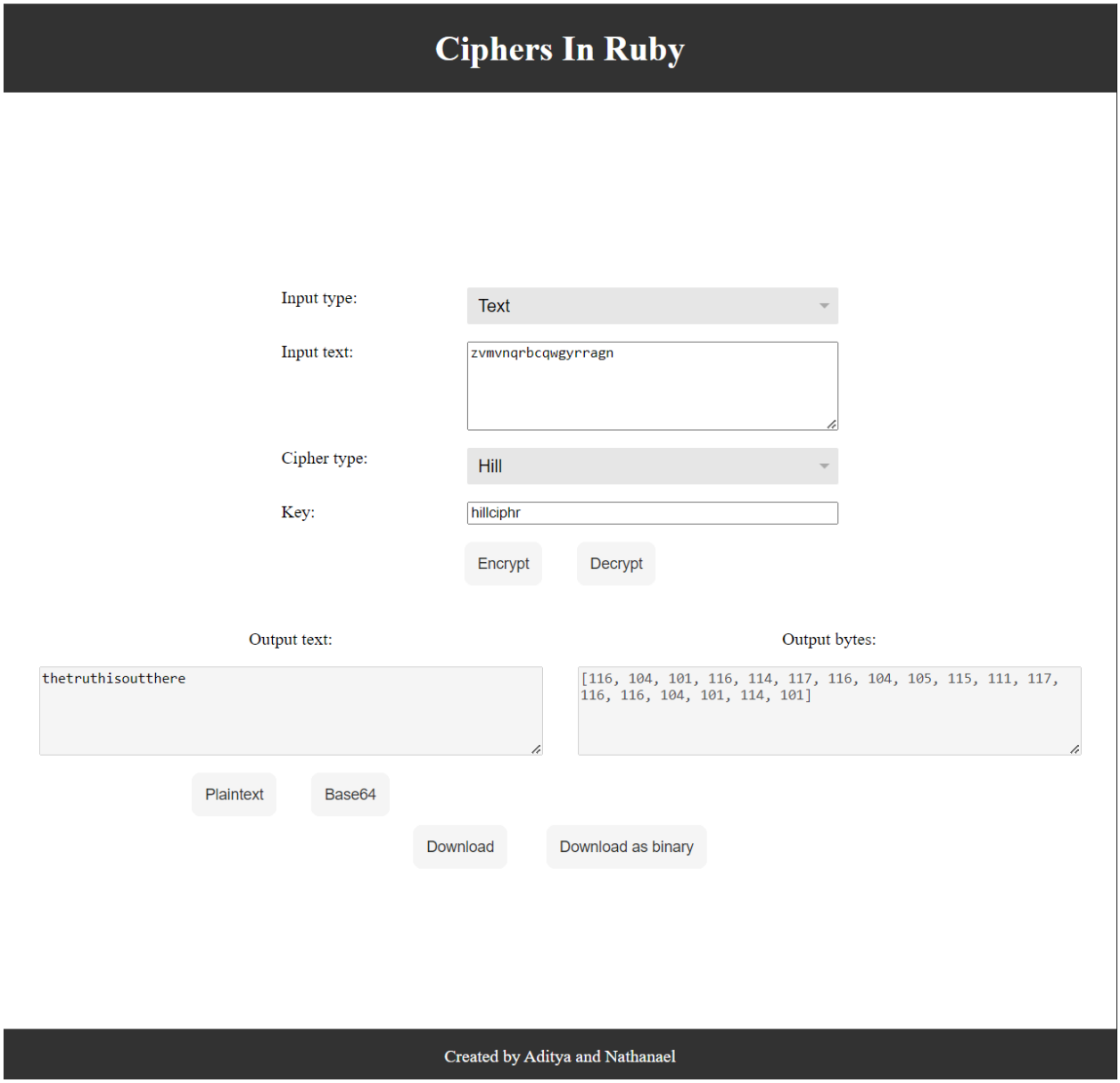
```
[122, 118, 109, 118, 110, 113, 114, 98, 99, 113, 119, 103,
121, 114, 114, 97, 103, 110]
```

Plaintext Base64

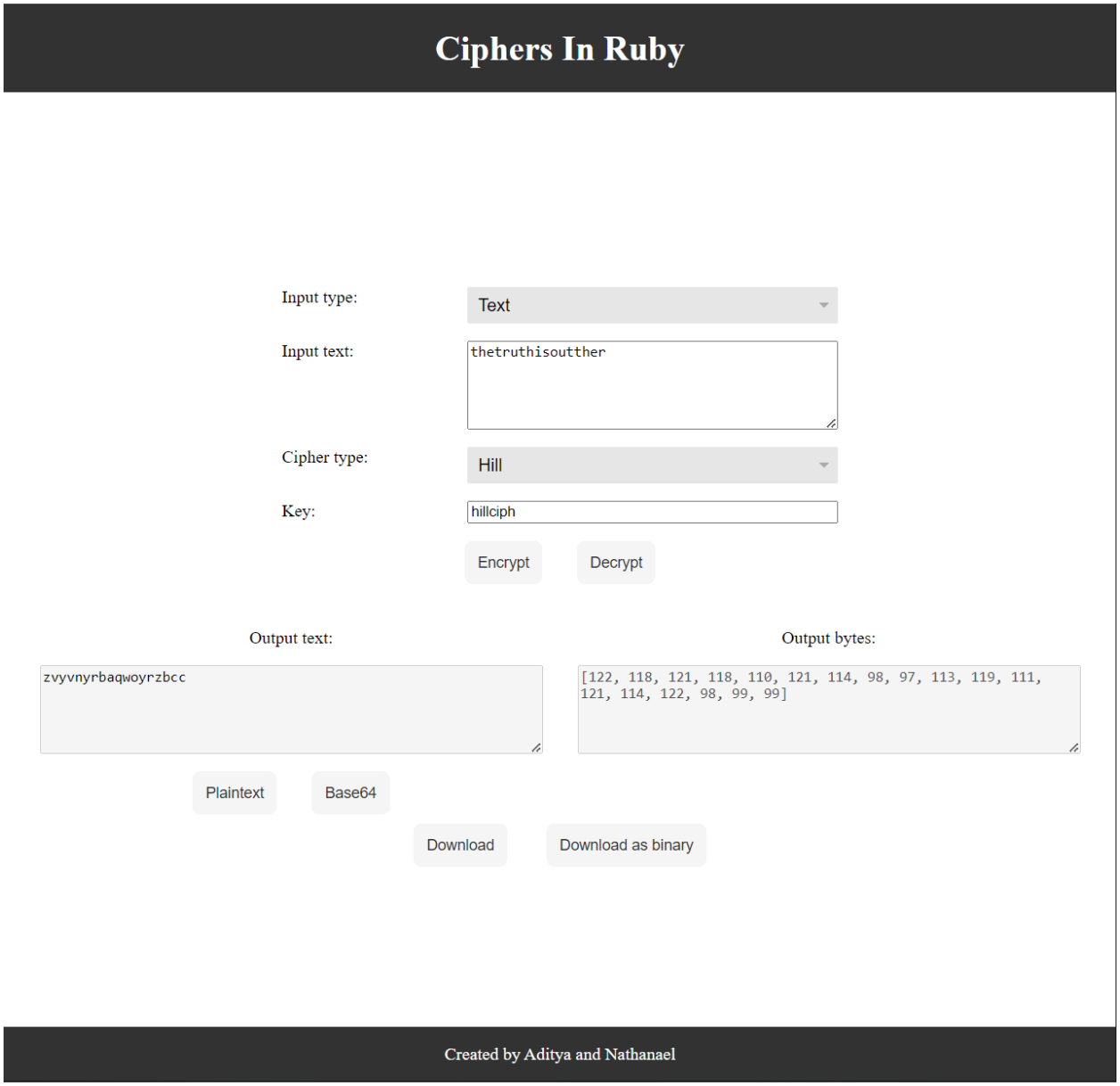
Download Download as binary



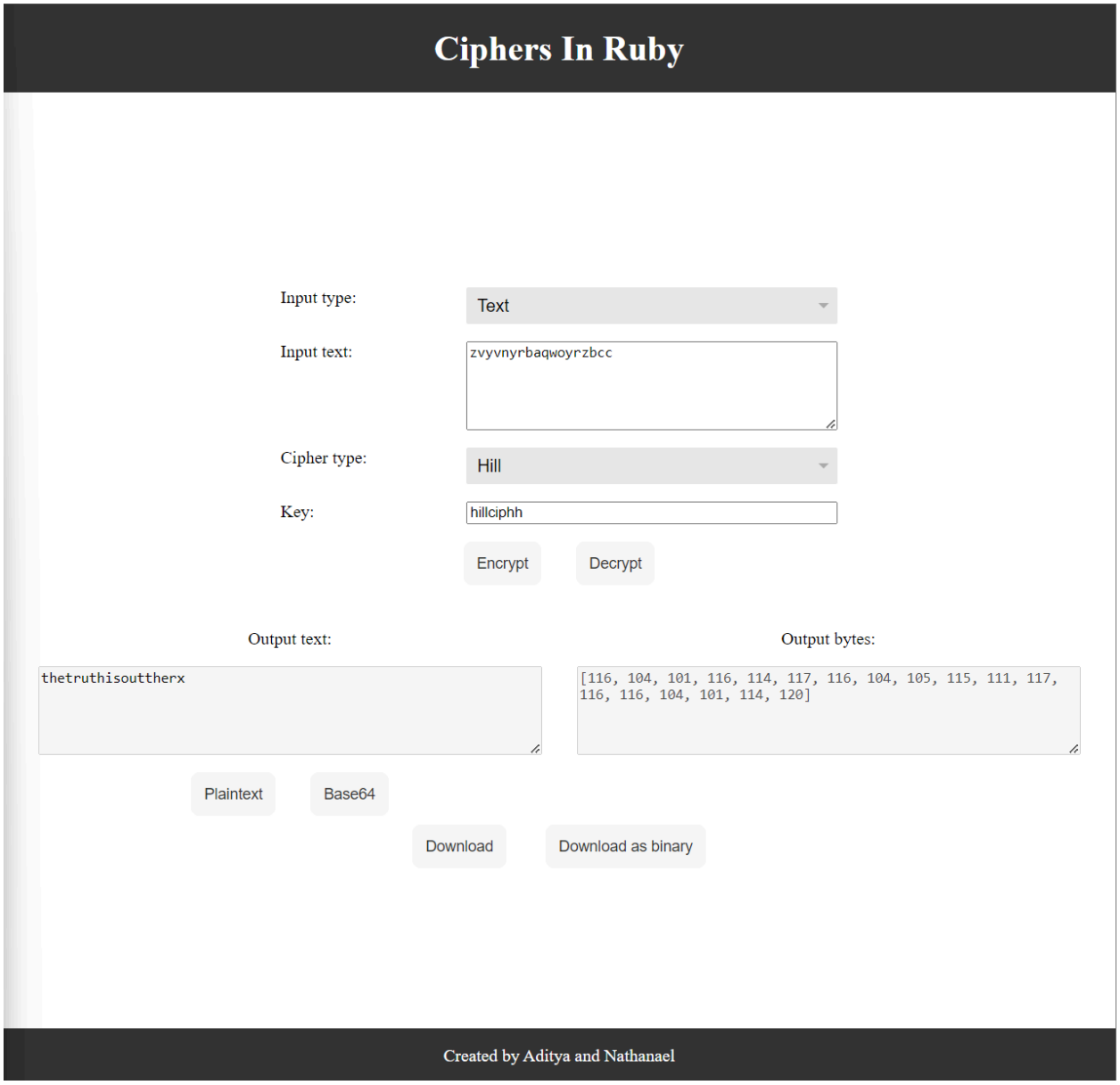
Hasil enkripsi plainteks “thetruthisoutthere” dengan kunci “hillciphr” dalam plainteks dan base64



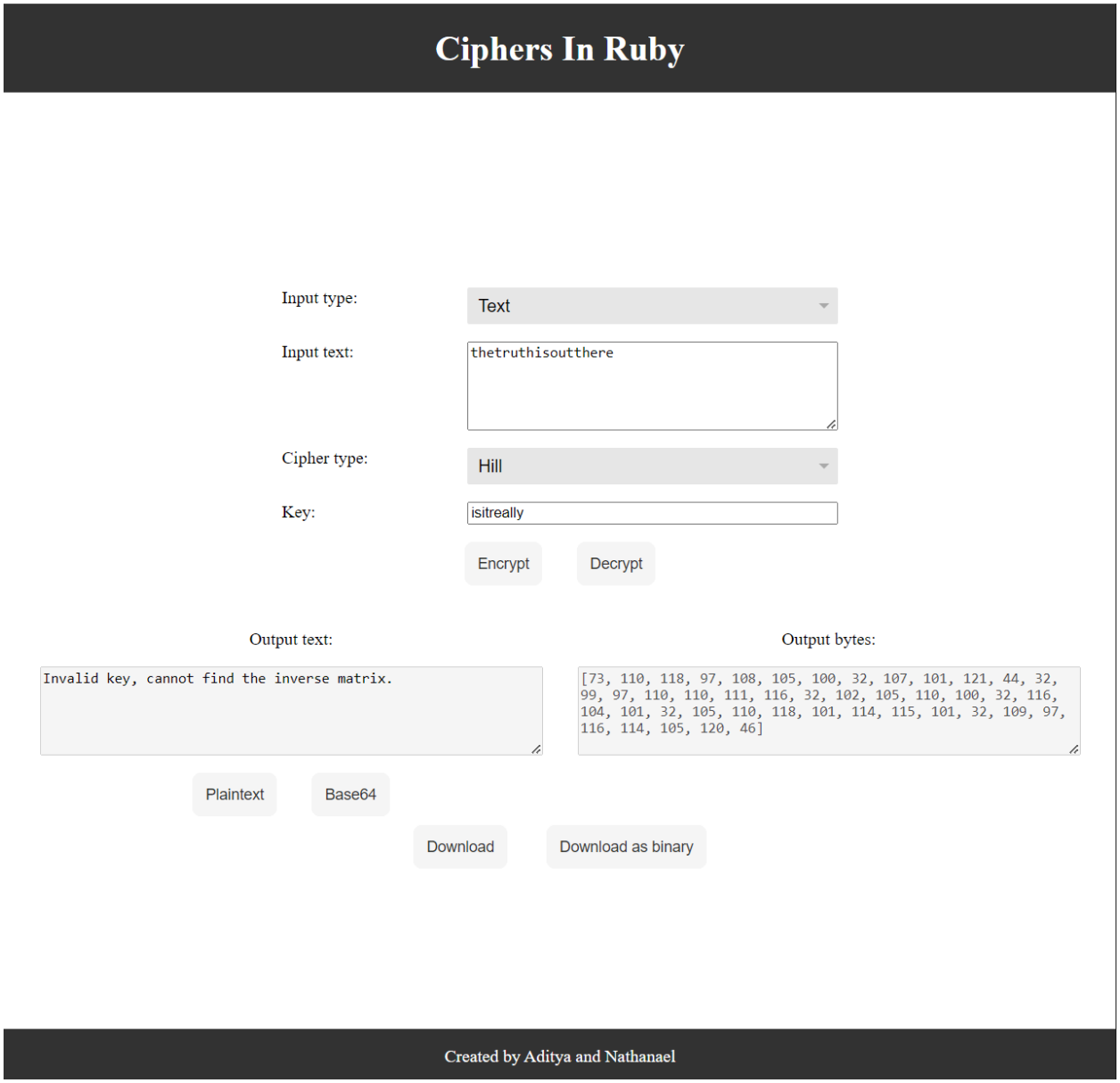
Hasil dekripsi plainteks “zvmvnqrbcqwgyrragn” dengan kunci “hillciphr”



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.

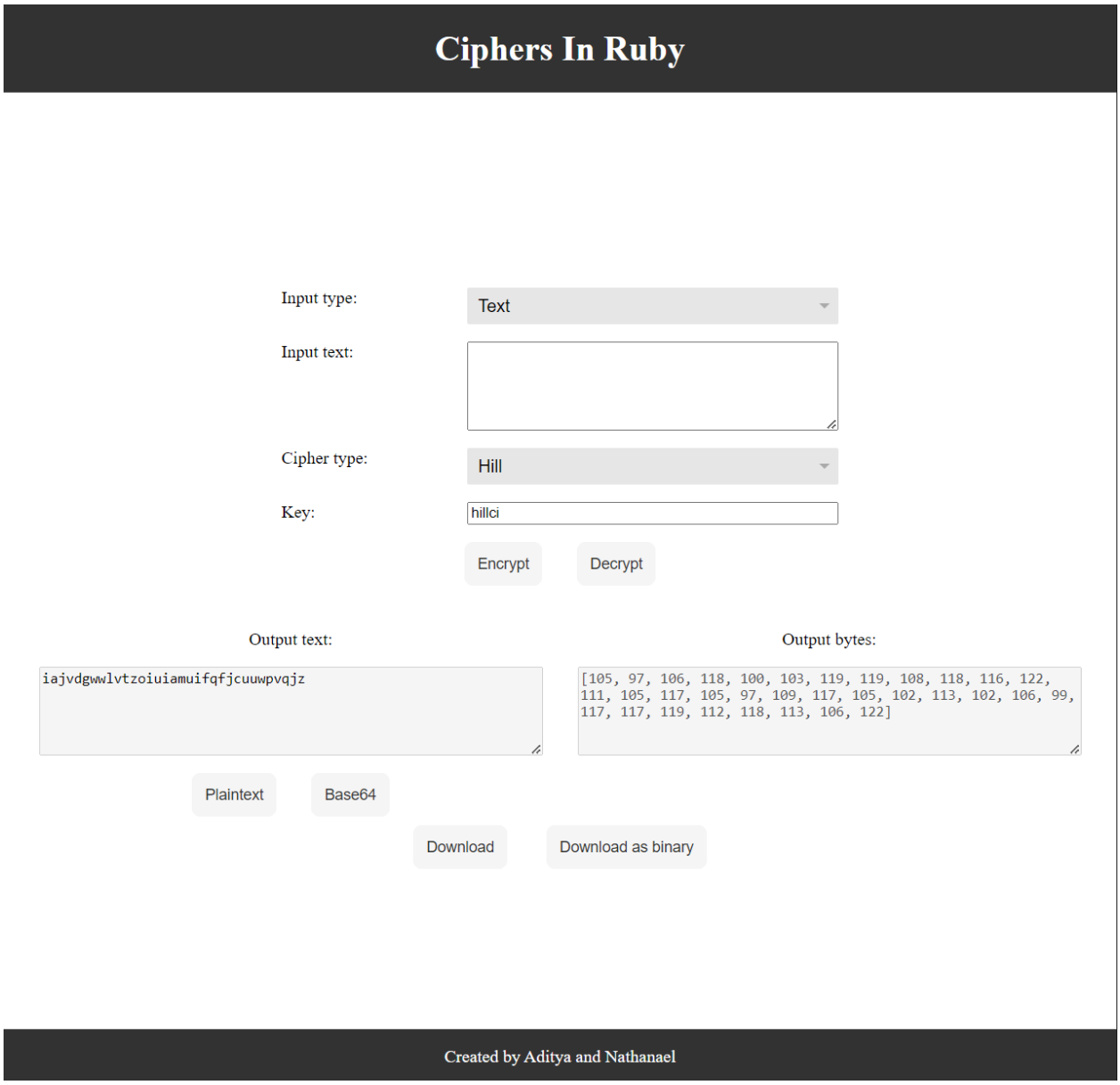


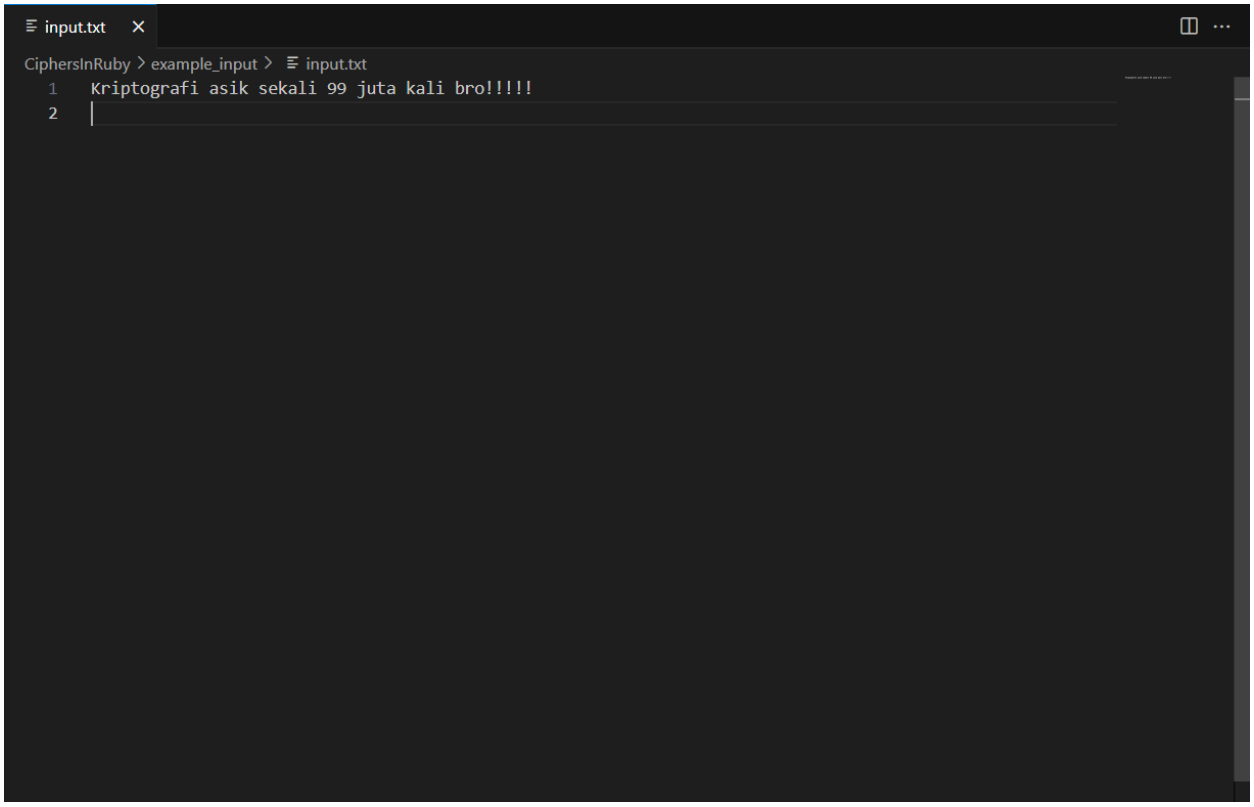
Hasil dekripsi plainteks “zvyvnyrbaqwoyrzbcc” dengan kunci “hillciphh” (hasil padding angka seeded random) yang menjadi “thetruthisouttherx” (di-pad “x”)

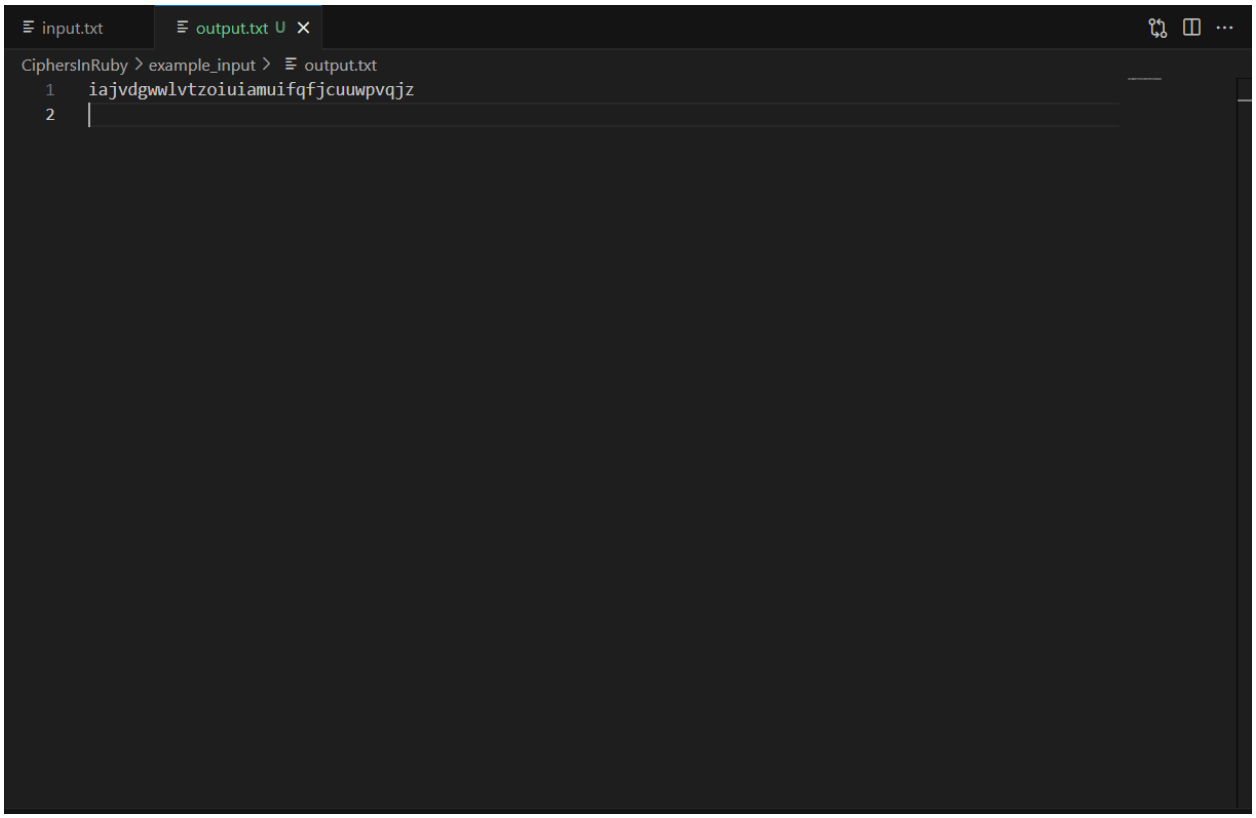


Hasil dekripsi plainteks “thetruthisoutthere” dengan kunci “isitreally” yang mengeluarkan invalid key error karena kunci tidak bisa mengasilkan modulo inverse matrix. Dengan kunci seperti ini, enkripsi akan tetap bisa dijalankan, hanya saja plainteks tersebut tidak bisa didekripsi.

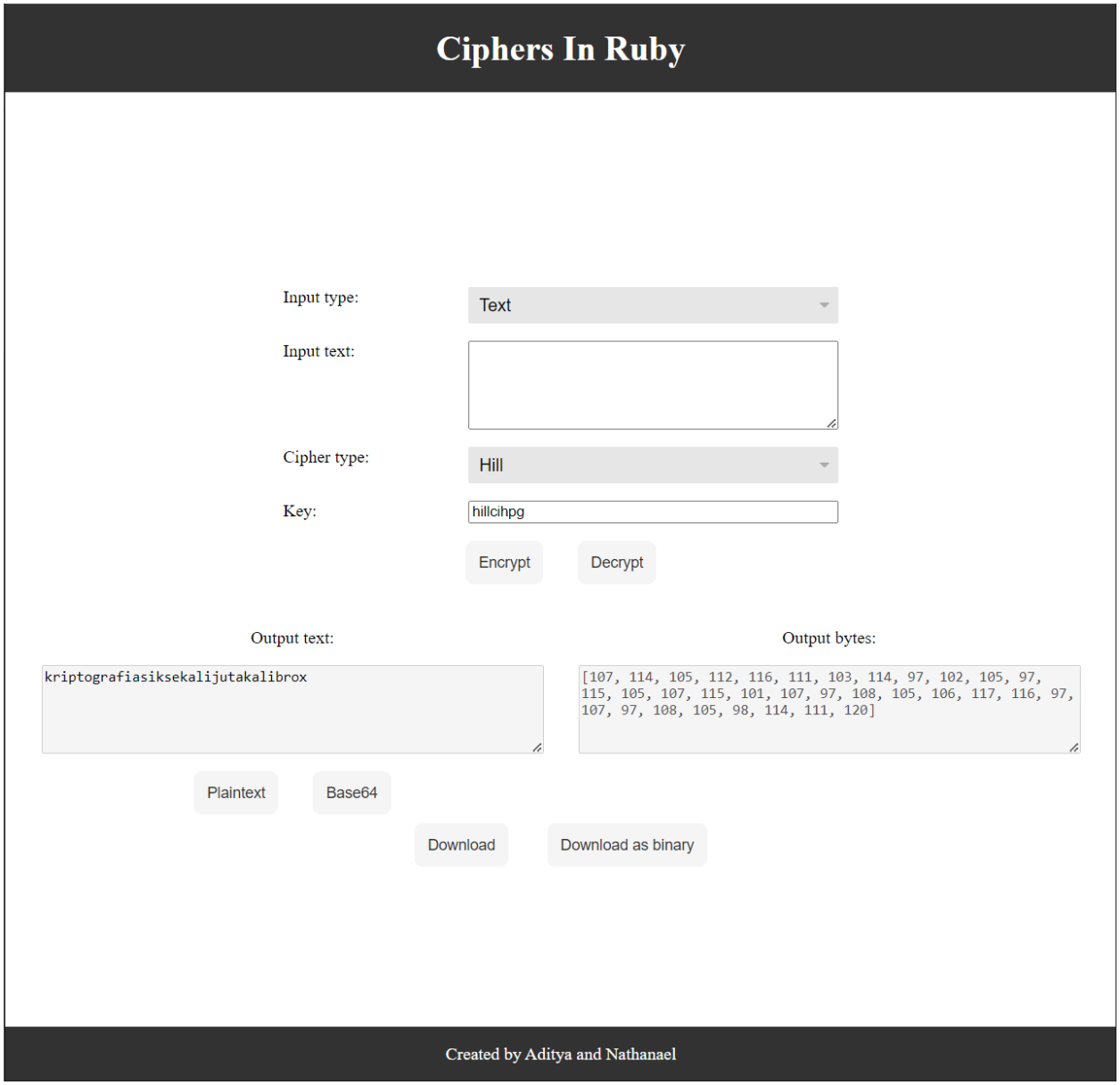
d. Input/Output File Teks “input.txt”







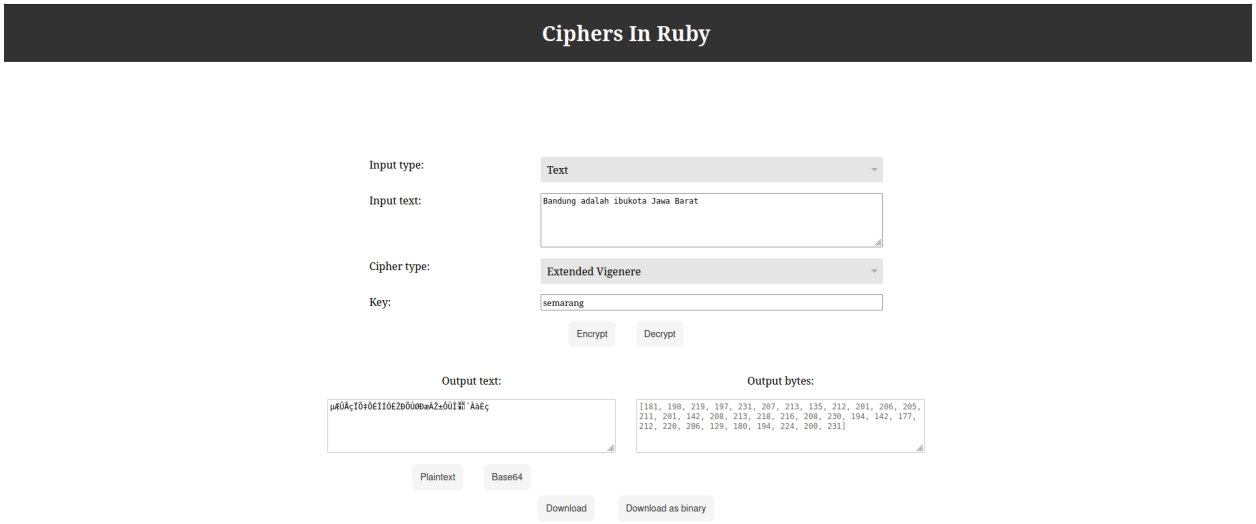
Hasil enkripsi *file* dengan kunci “hillci” dalam bentuk file “output.txt”



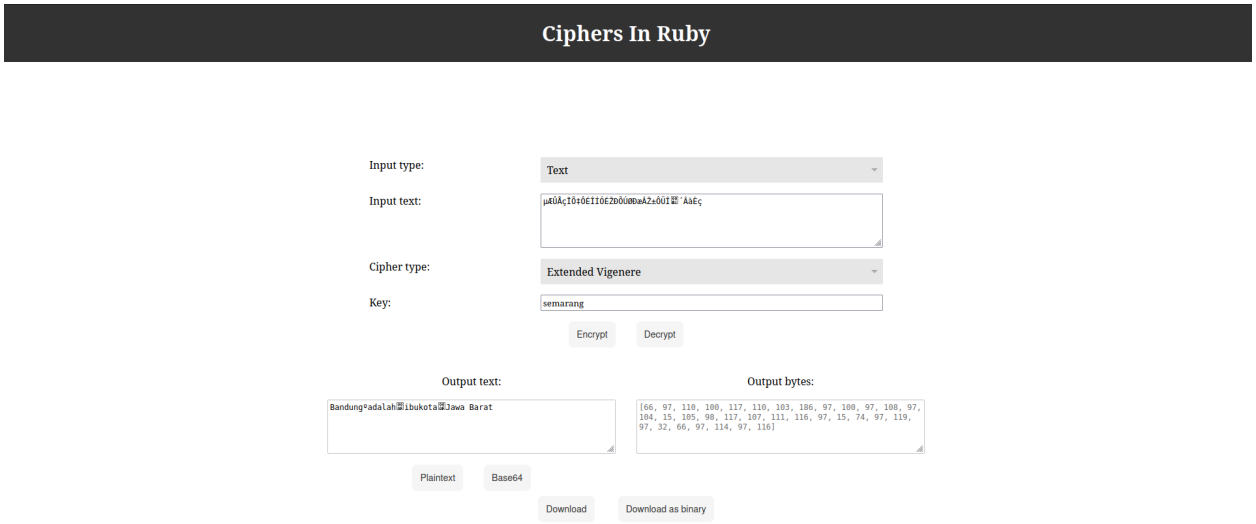
Hasil dekripsi *file* “output.txt” dalam bentuk plainteks dengan kunci “hillcihpg” (hasil seeded random padding). Keluaran ada padding ‘x’

6. *Extended* Vigenere Cipher

1. Input/Output Plainteks

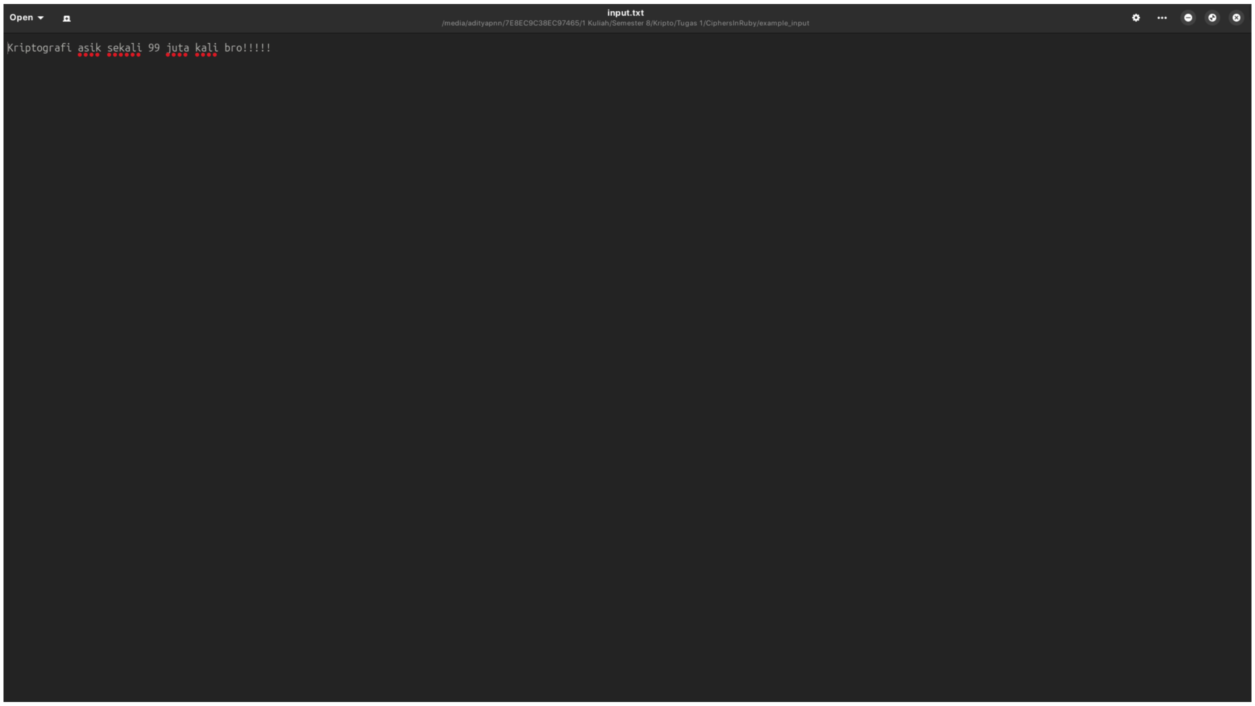


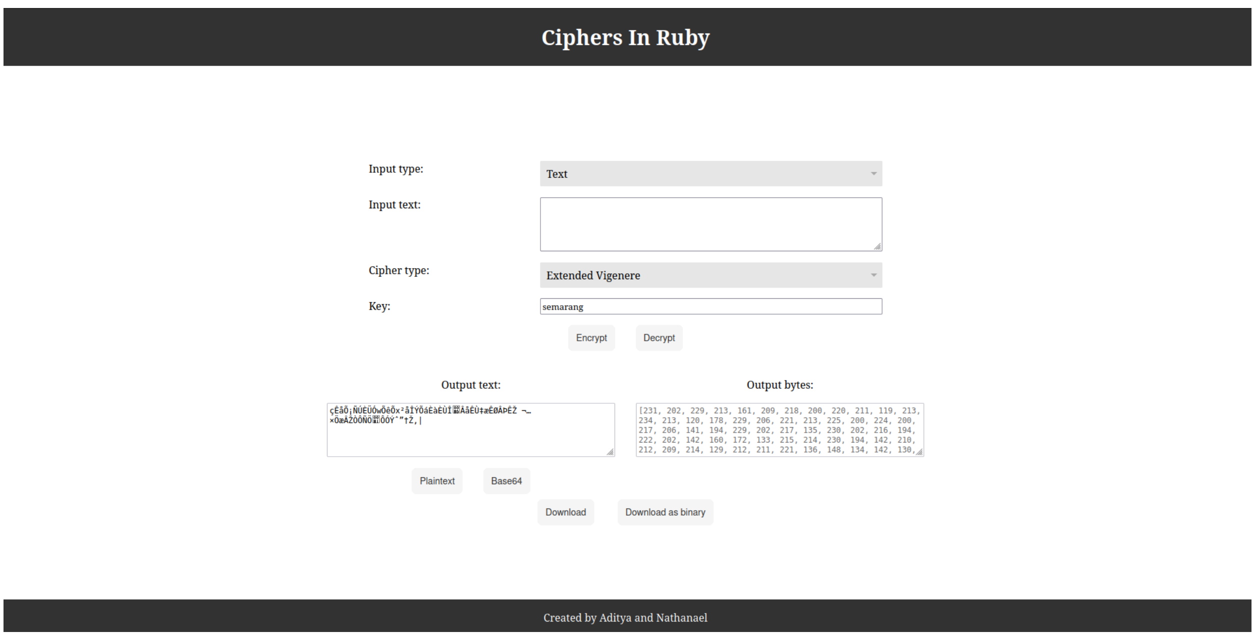
Hasil enkripsi “Bandung adalah ibukota Jawa Barat” dengan kunci “semarang”

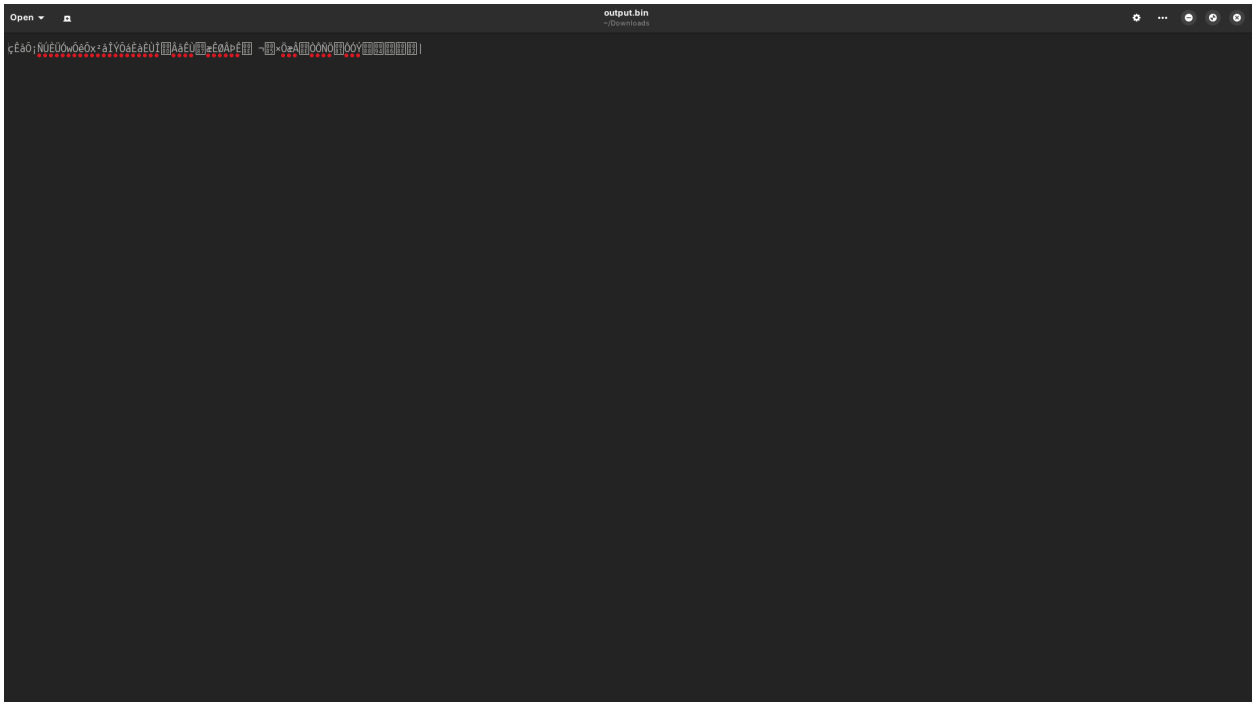


Hasil dekripsi dari cipherteks menunjukkan karakter yang rusak. Hal ini dikarenakan dalam bahasa Ruby, pembaca byte beberapa karakter spesial didasarkan pada *encoding* “UTF-8” sehingga hasil pembacaan dalam integer melebihi 255 (jumlah karakter ASCII).

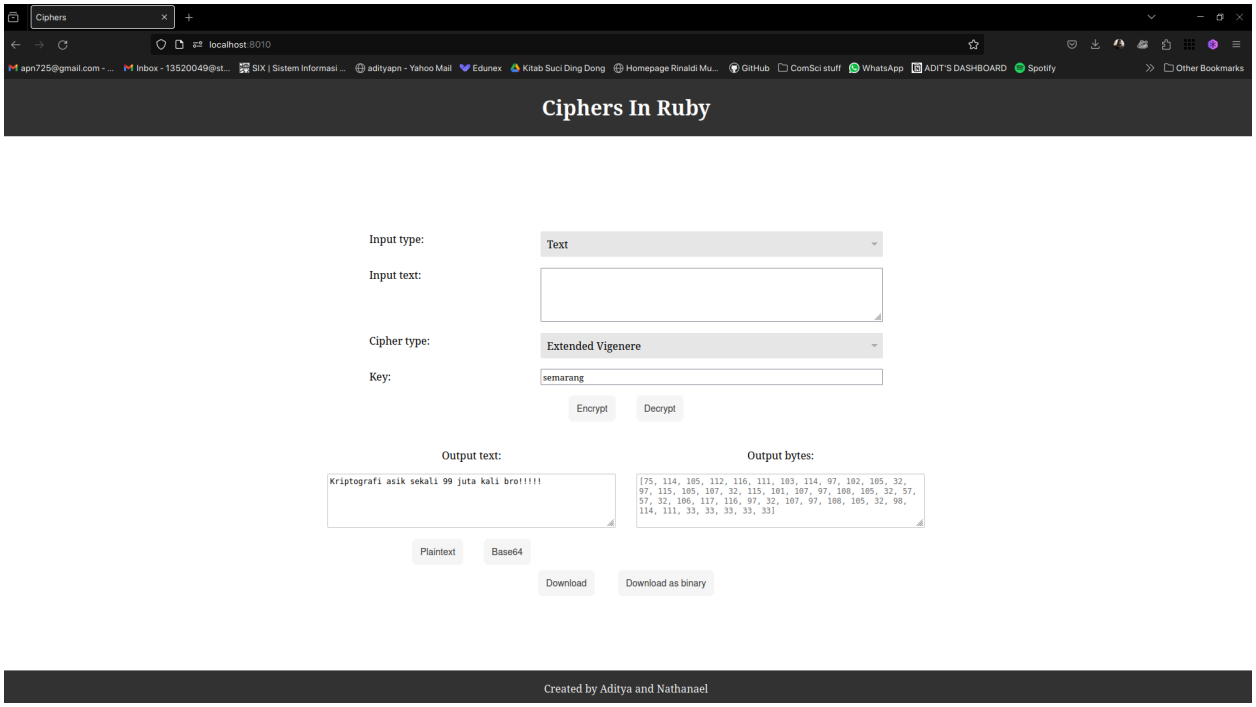
2. Input/Output File Teks “input.txt”

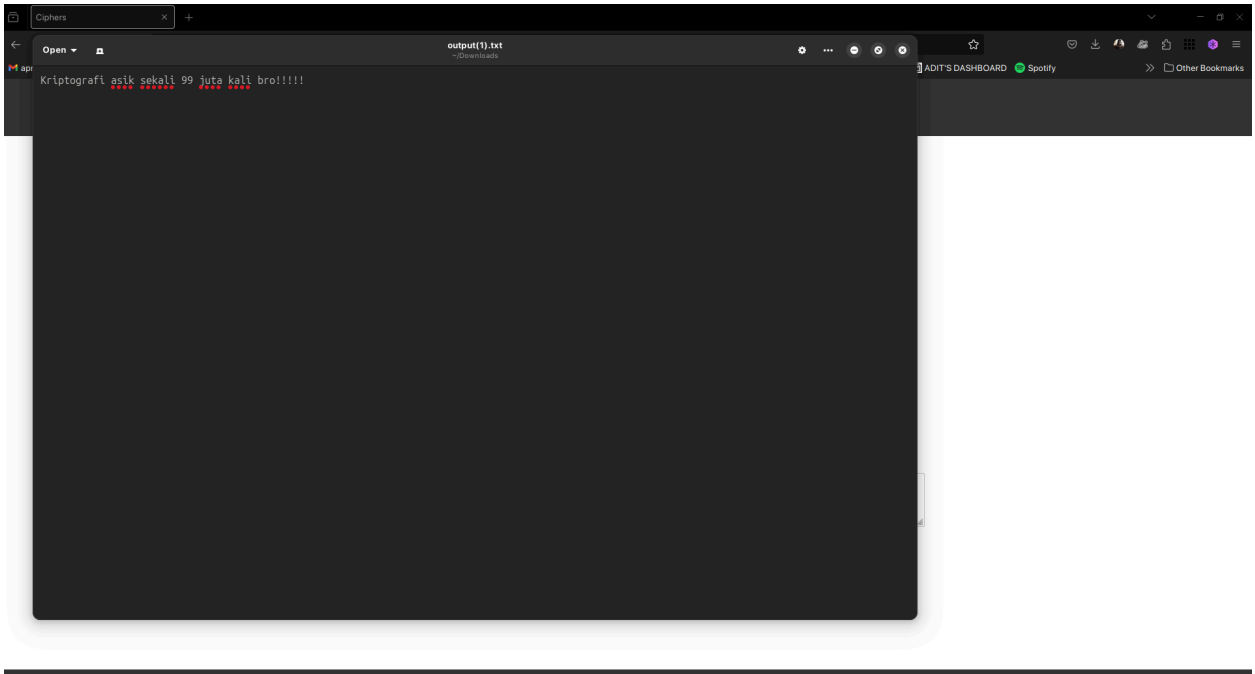

Open
input.txt
Kriptografi asik sekali 99 juta kali bro!!!!!


Ciphers In Ruby
Input type:
Text
Input text:
Cipher type:
Extended Vigenere
Key:
semarang
Encrypt
Decrypt
Output text:
Output bytes:
[231, 202, 229, 213, 161, 209, 218, 200, 220, 211, 119, 213, 234, 213, 120, 178, 229, 206, 221, 213, 225, 200, 224, 200, 217, 206, 141, 194, 229, 202, 217, 135, 230, 202, 216, 194, 222, 202, 142, 160, 172, 133, 215, 214, 230, 194, 142, 210, 212, 209, 214, 129, 212, 211, 221, 136, 148, 134, 142, 130,
Plaintext
Base64
Download
Download as binary
Created by Aditya and Nathanael



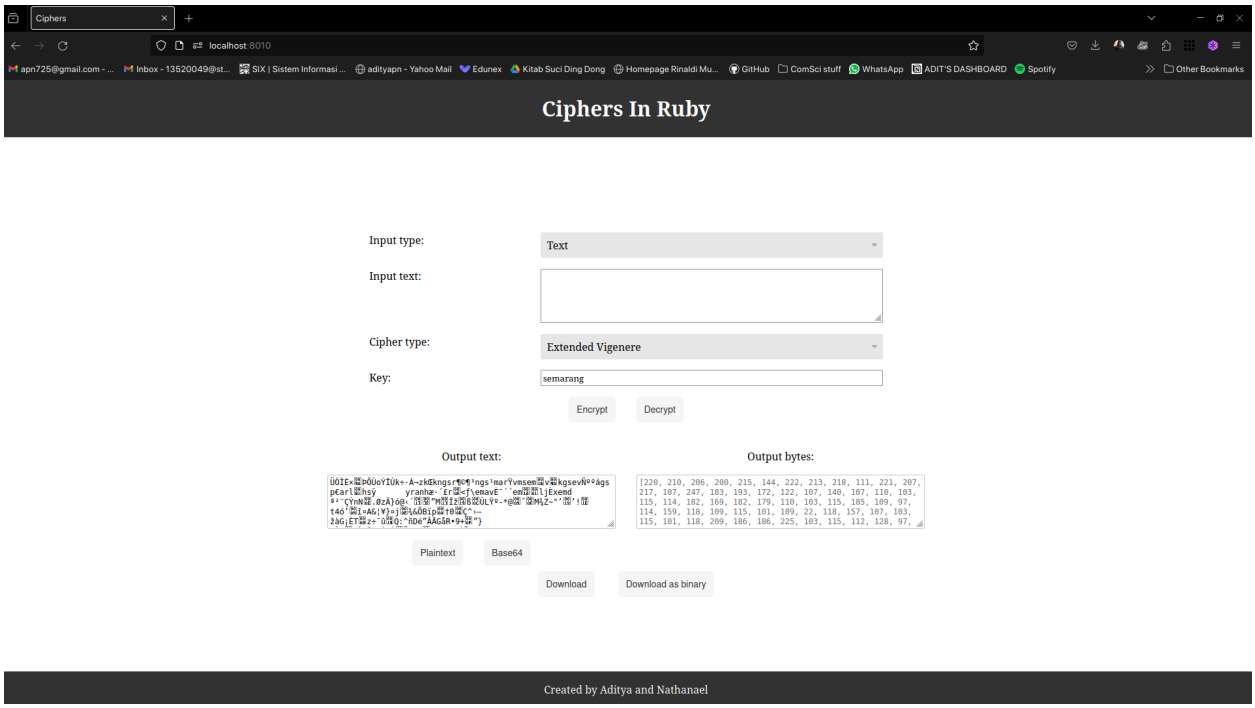
Hasil enkripsi dengan kunci “semarang” dari file yang diunduh dalam bentuk file *binary*.

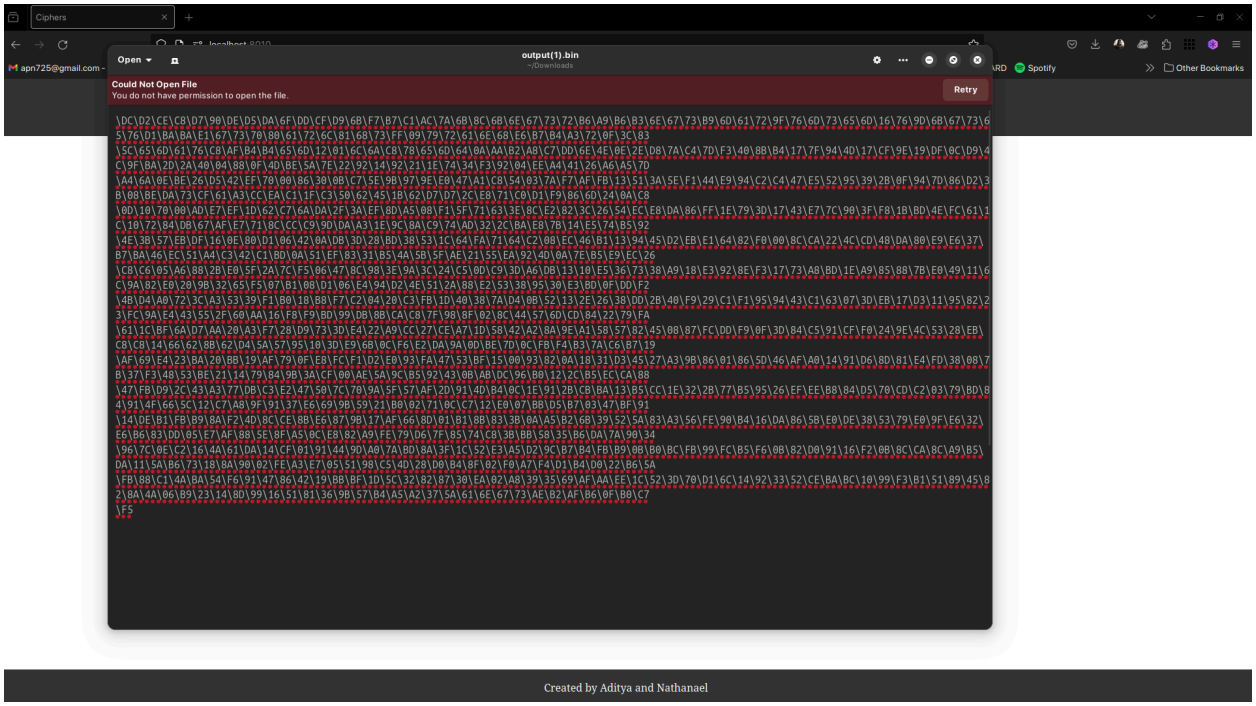




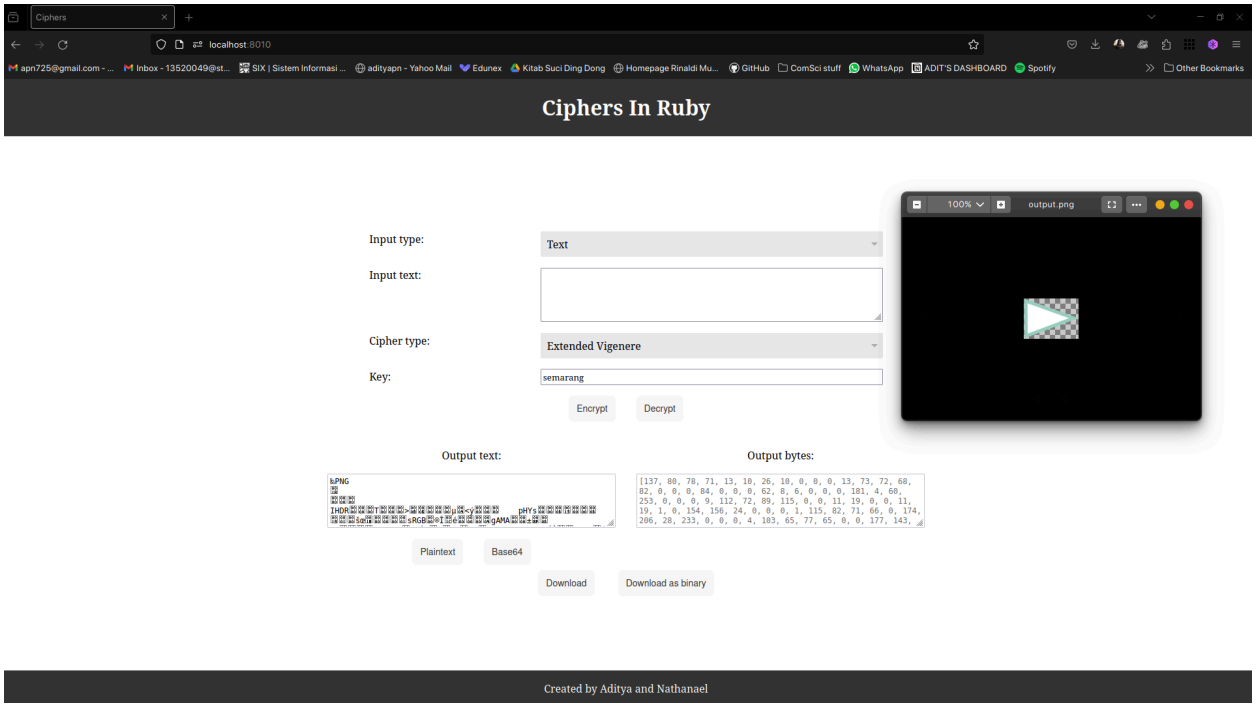
Hasil dekripsi file “output.bin” dengan kunci “semarang” dalam bentuk plainteks dan file semula.

3. Input/Output File Teks “input.png”



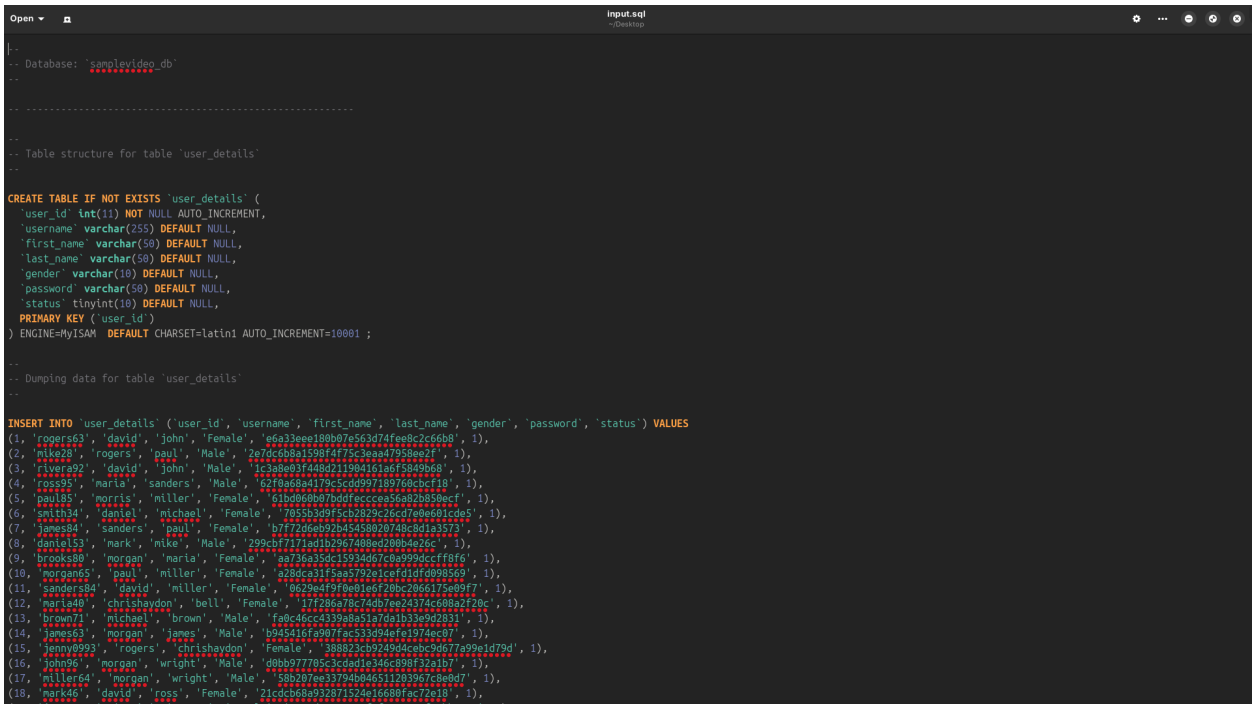


Hasil enkripsi gambar dengan kunci “semarang” dalam bentuk plainteks dan binary.

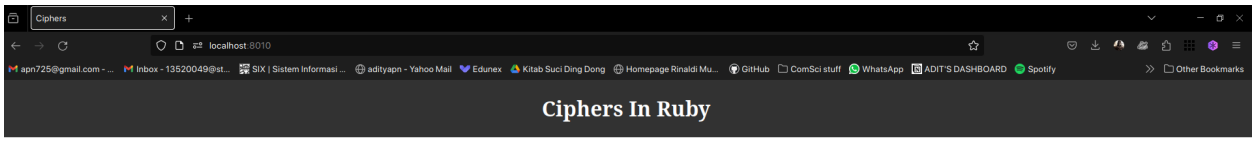


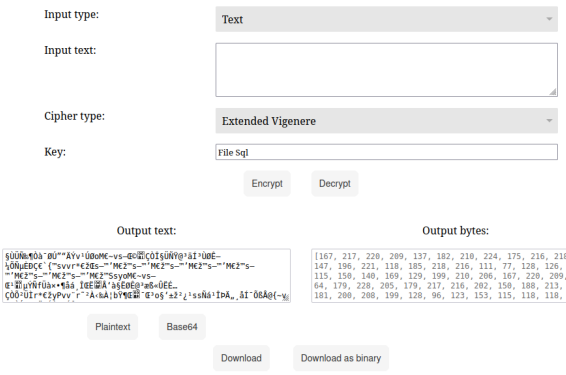
Hasil dekripsi file *binary* dengan kunci “semarang” yang diunduh dengan ekstensi file sesuai dan plainteks.

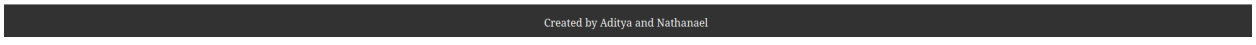
4. Input/Output File Teks “input.sql”

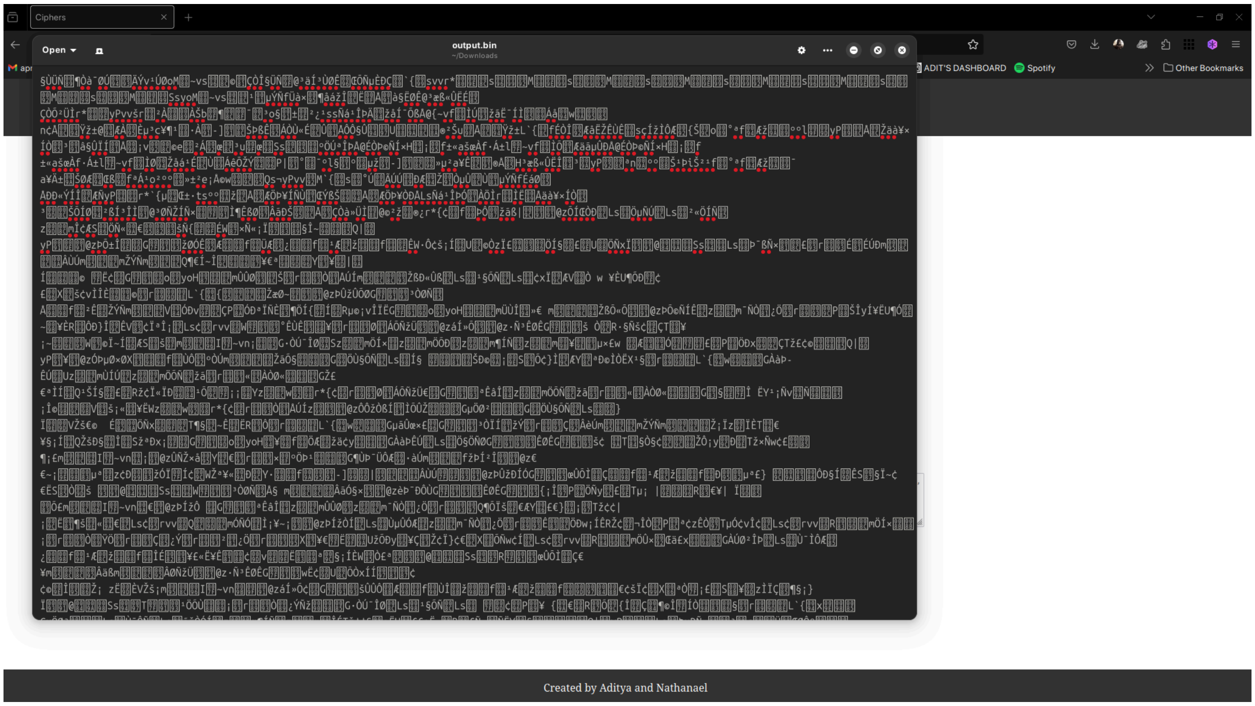


```
Open ▾   input.sql   ~/Desktop

--
-- 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, 'rogers63', 'david', 'john', 'Female', 'e6a33eee180b07e563d74fee8c2c66b8', 1),
(2, 'mike28', 'rogers', 'paul', 'Male', '2e7dc6b8a1598f4f75c3eaa47958ee2f', 1),
(3, 'rivera92', 'david', 'john', 'Male', '1c3a8e03f448d2119041 61a6f5849b68', 1),
(4, 'ross95', 'maria', 'sanders', 'Male', '62f0a68a4179c5cdd997189760cbcf18', 1),
(5, 'paul85', 'morris', 'miller', 'Female', '61bd060b07bdfeccceae56a82b858ecf', 1),
(6, 'smith34', 'daniel', 'michael', 'Female', '7055b3d9f5cb2829c26cdfe0e601cde5', 1),
(7, 'james84', 'sanders', 'paul', 'Female', 'b7f72d6eb92b4545802074 8c01a35f3', 1),
(8, 'daniel53', 'mark', 'mike', 'Male', '299cbf7171ad1b2967408ed2 00b4e26c', 1),
(9, 'brooks80', 'morgan', 'maria', 'Female', 'ae736a35dc15934d67c0a999dccff8f6', 1),
(10, 'morgan65', 'paul', 'miller', 'Female', 'a28dca31f5aa5792e1cefd1dfd098569', 1),
(11, 'sanders84', 'david', 'miller', 'Female', '0629e4f9f0e01e6f20bc2066175e09f7', 1),
(12, 'maria40', 'chrishaydon', 'bell', 'Female', '17f286a78c74db7ee24374c608a2f20c', 1),
(13, 'brown71', 'michael', 'brown', 'Male', 'fa0c46cc4339a8a51a7da1b33e9d2831', 1),
(14, 'james63', 'morgan', 'james', 'Male', 'b945416fa907fac533d94efe1974ec07', 1),
(15, 'jenny0993', 'rogers', 'chrishaydon', 'Female', '388823cb9249d4cebc9d677a99e1d79d', 1),
(16, 'john96', 'morgan', 'wright', 'Male', 'd0bb977705c3cdad1e346c898f32a1b7', 1),
(17, 'miller64', 'morgan', 'wright', 'Male', '58b207ee33794b046511203967c8e0d7', 1),
(18, 'mark46', 'david', 'ross', 'Female', '21cdcb68a932871524e16680fac72e18', 1),
```

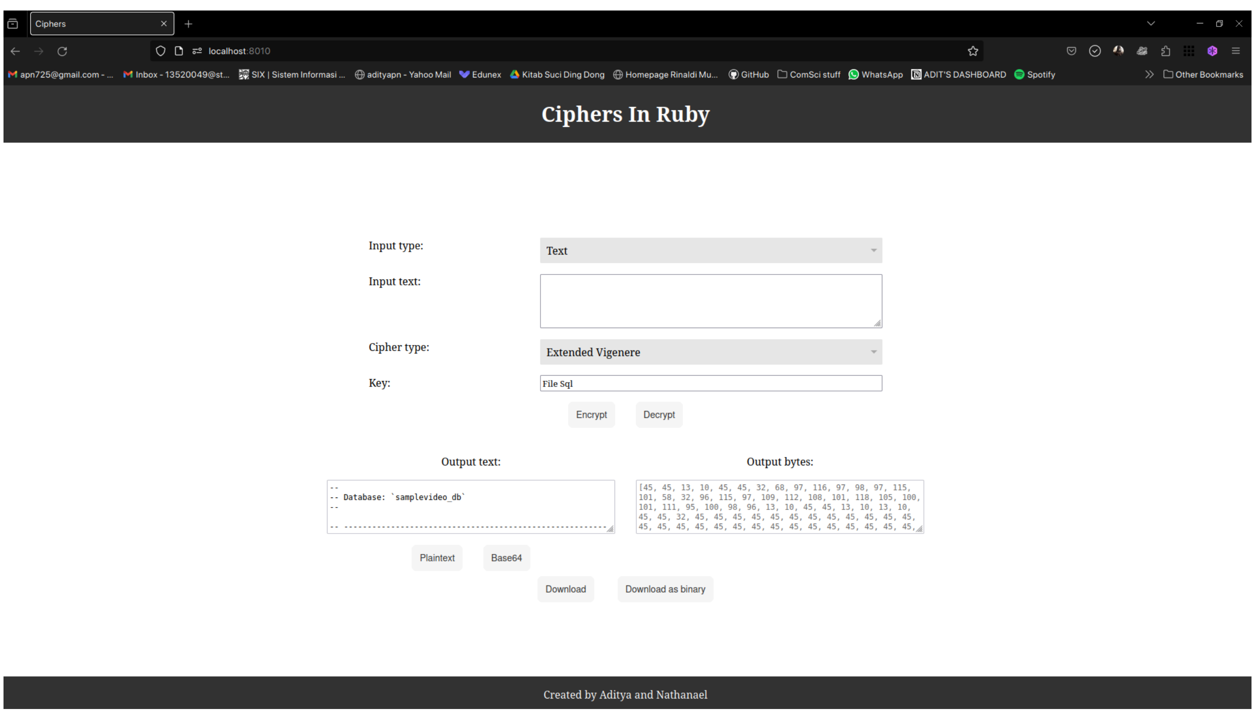


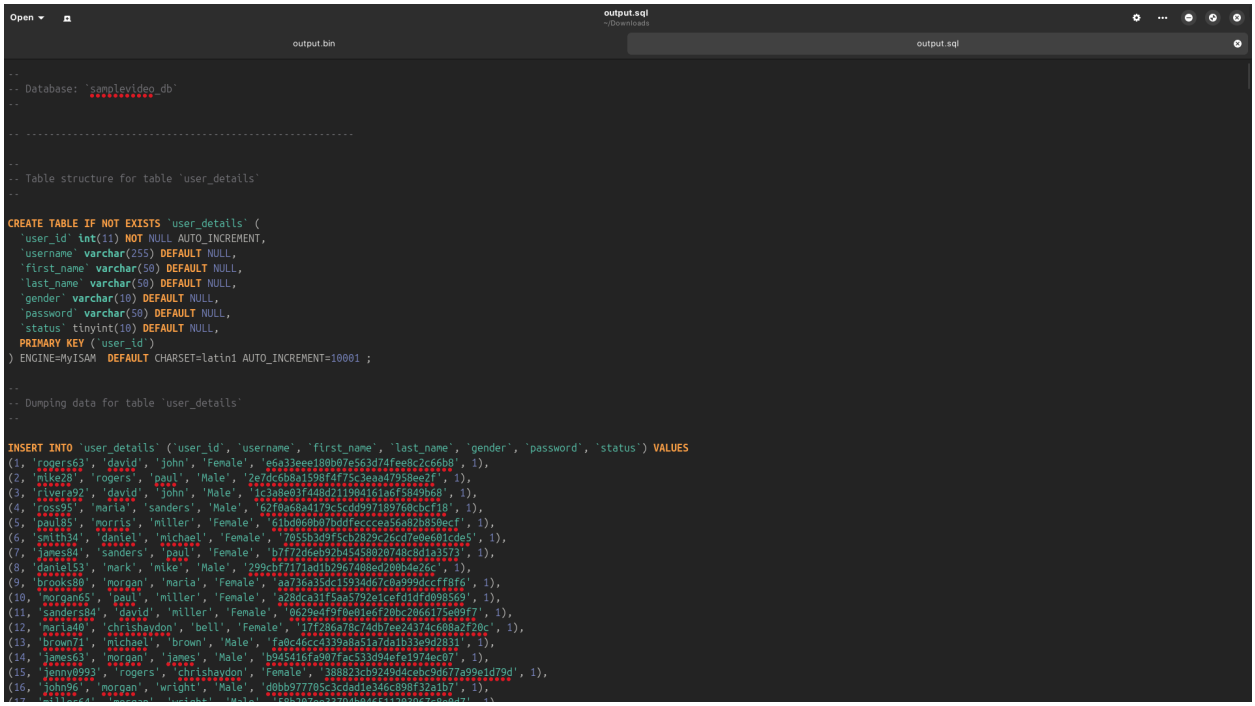






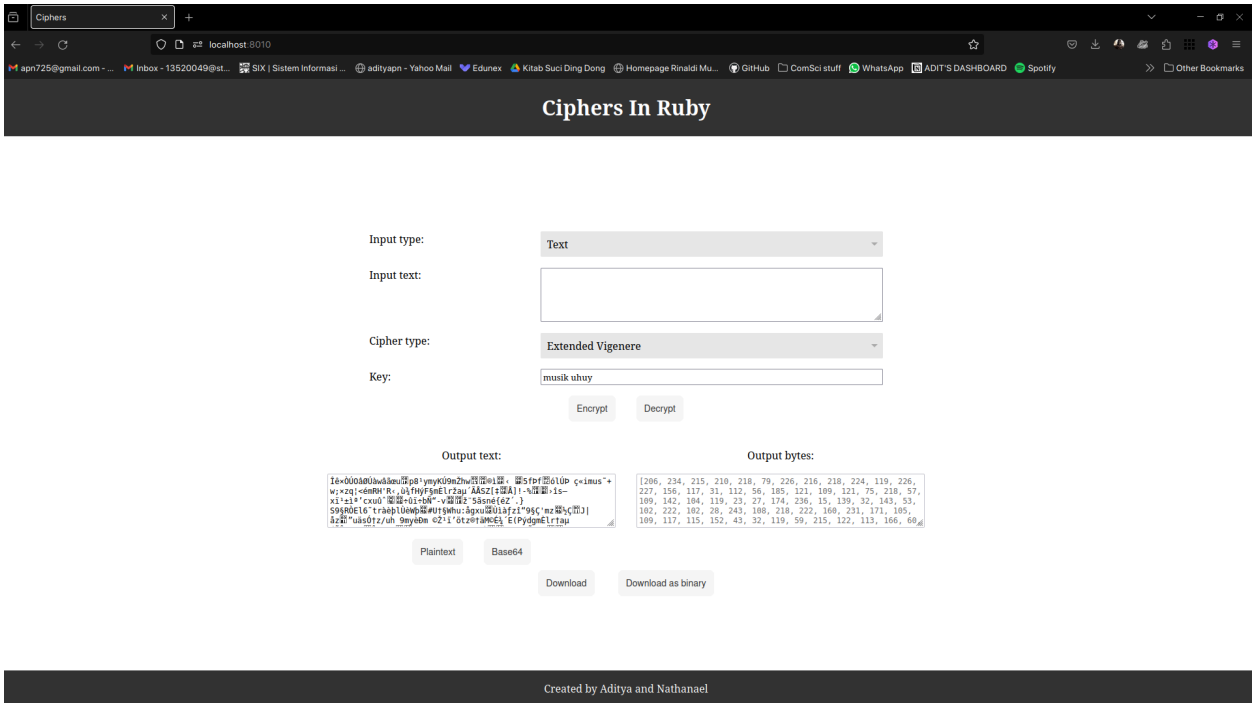
Hasil enkripsi file input.sql dengan kunci “File Sql” ke dalam bentuk binary dan plainteks



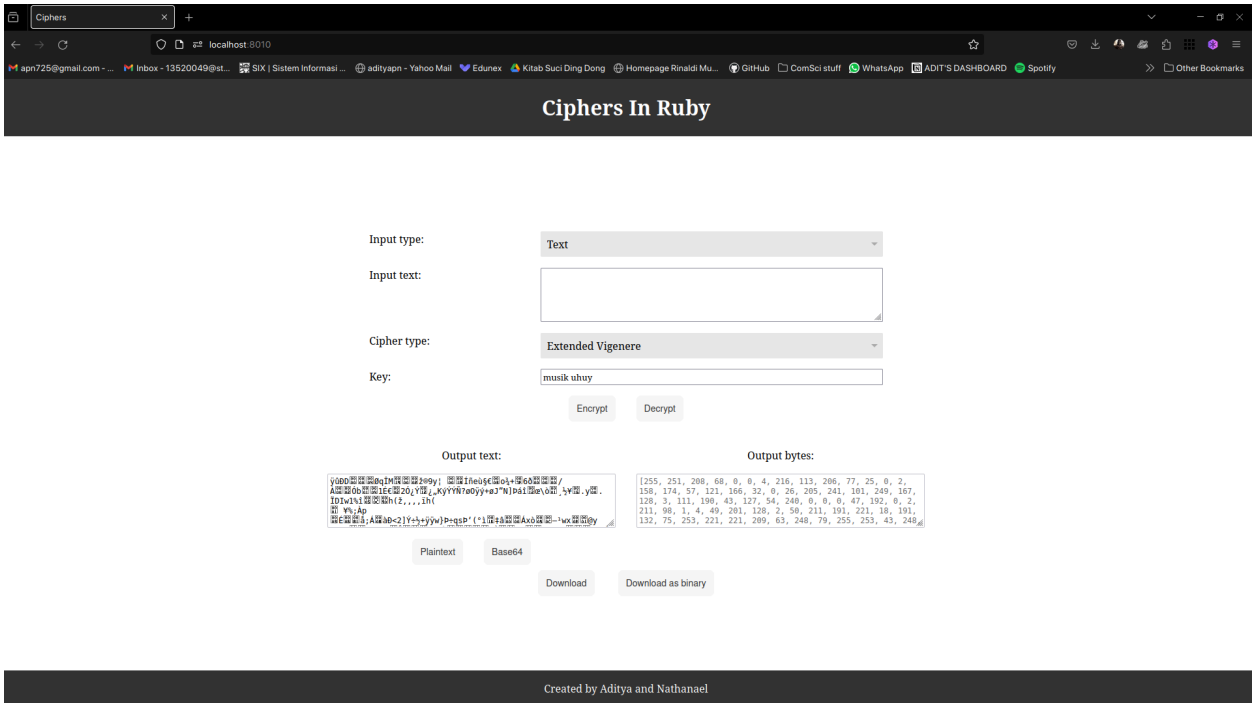


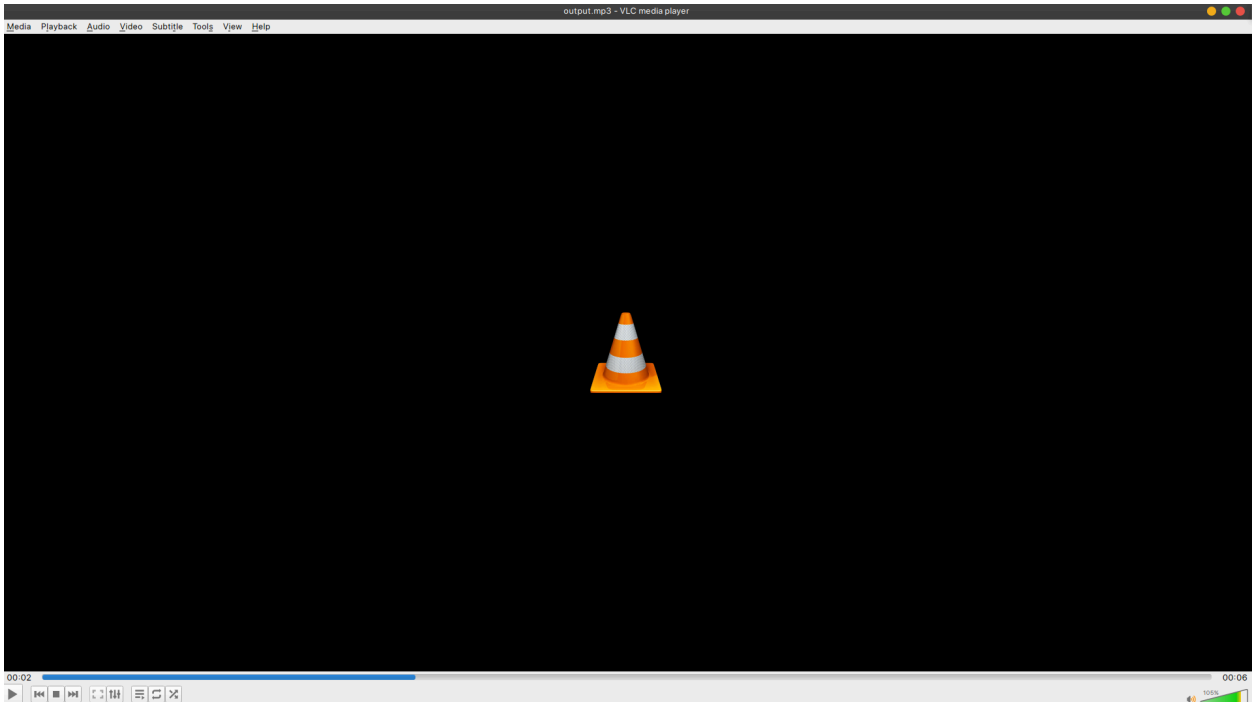
Hasil dekripsi file binary dengan kunci “File Sql” dalam bentuk plainteks dan file sql

5. Input/Output File Teks “input.mp3”



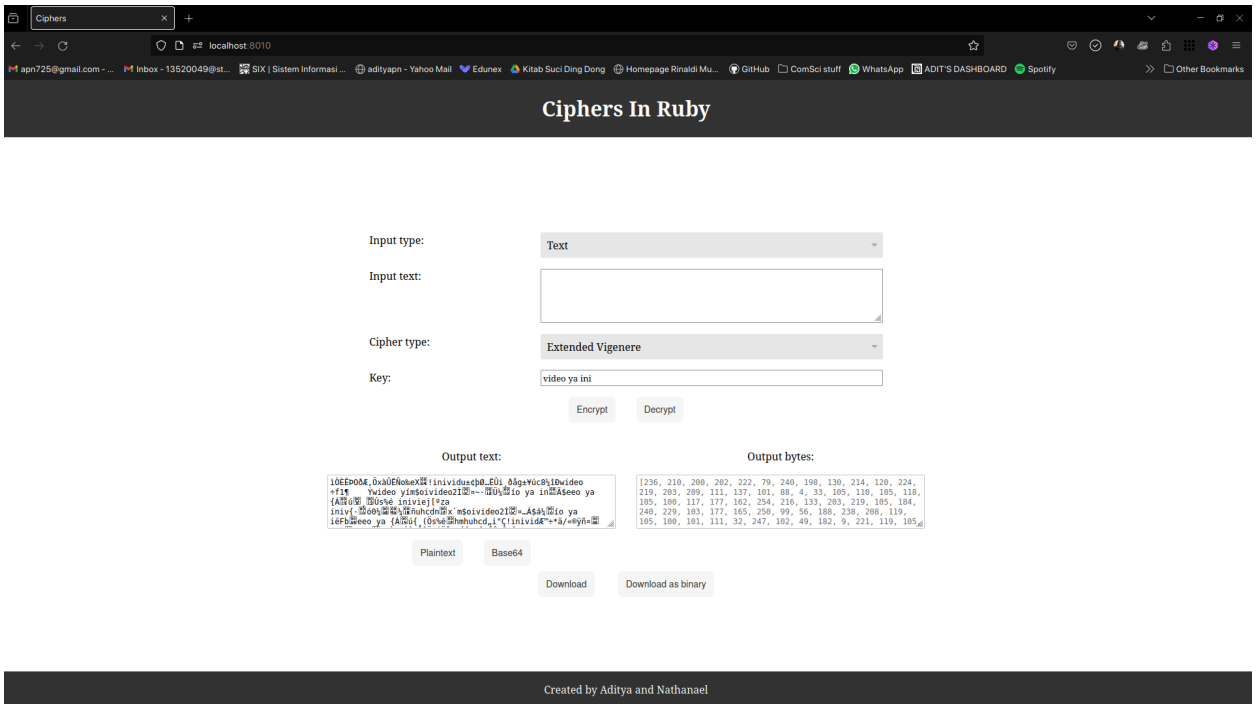
Hasil enkripsi file mp3 dengan kunci “musik uhuy” dalam bentuk plainteks dan binary

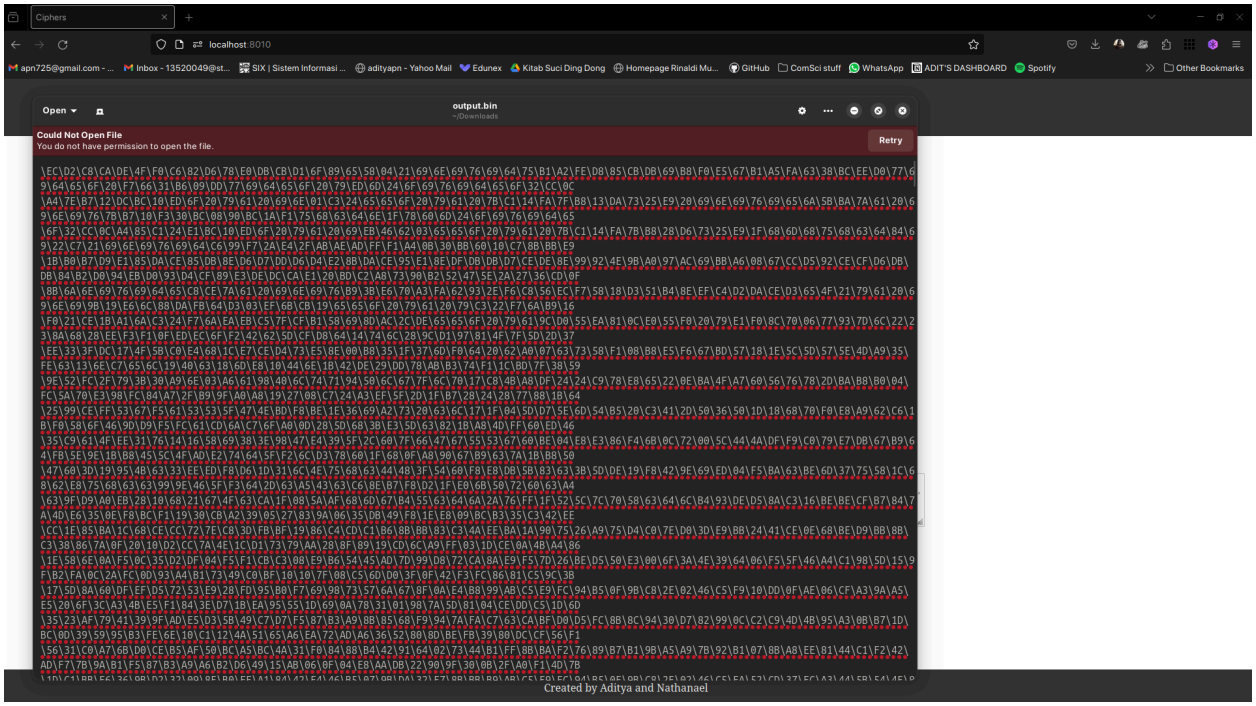




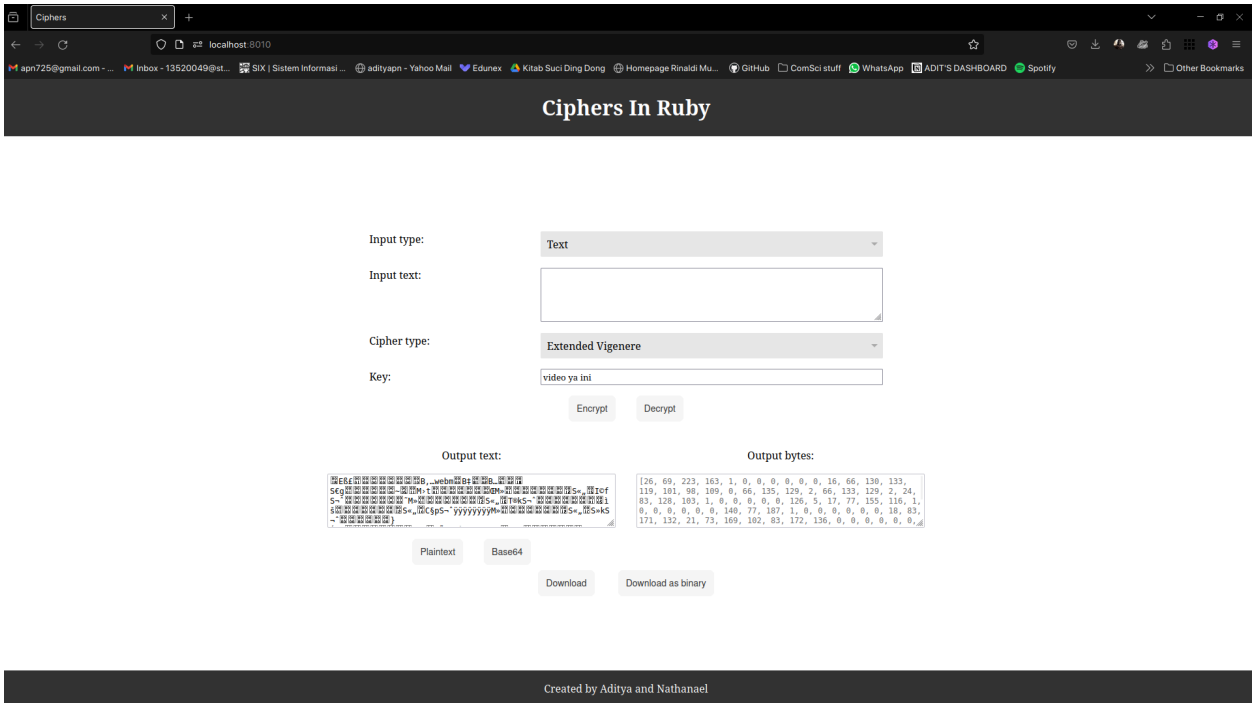
Hasil dekripsi file output(1).bin dengan kunci “musik uhuy” dalam bentuk plainteks dan ekstensi file mp3

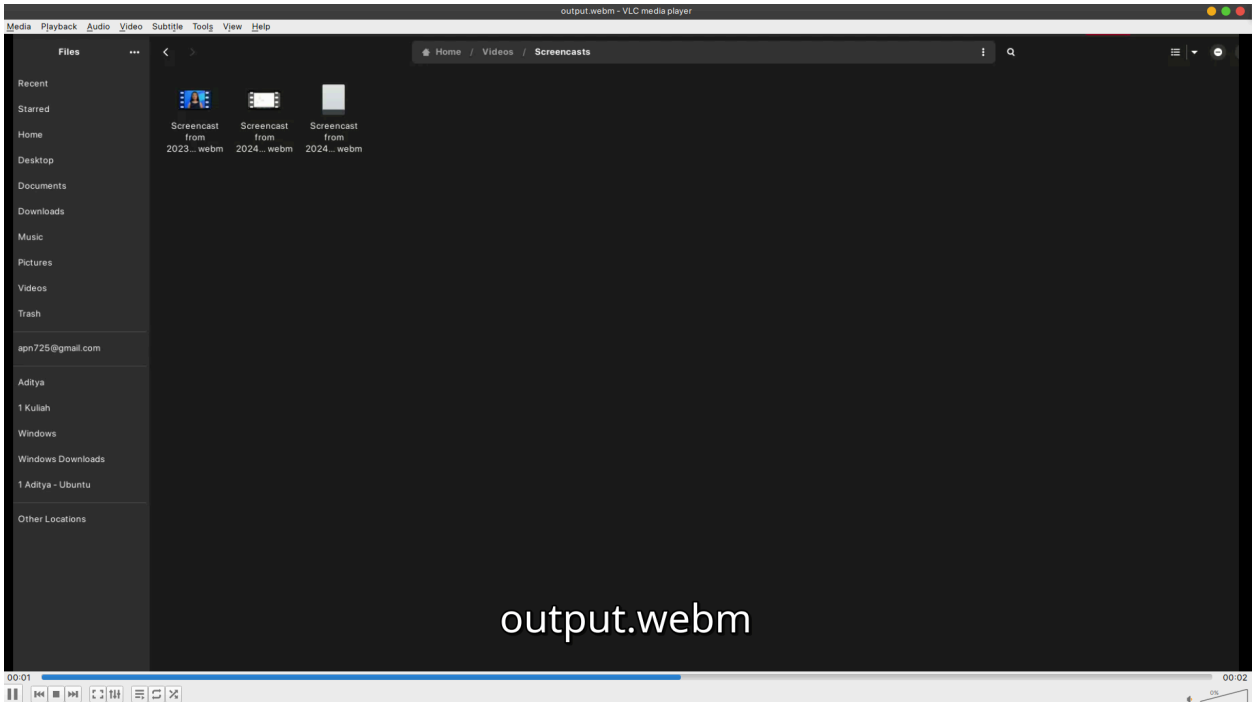
6. Input/Output File Teks “input.webm”





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

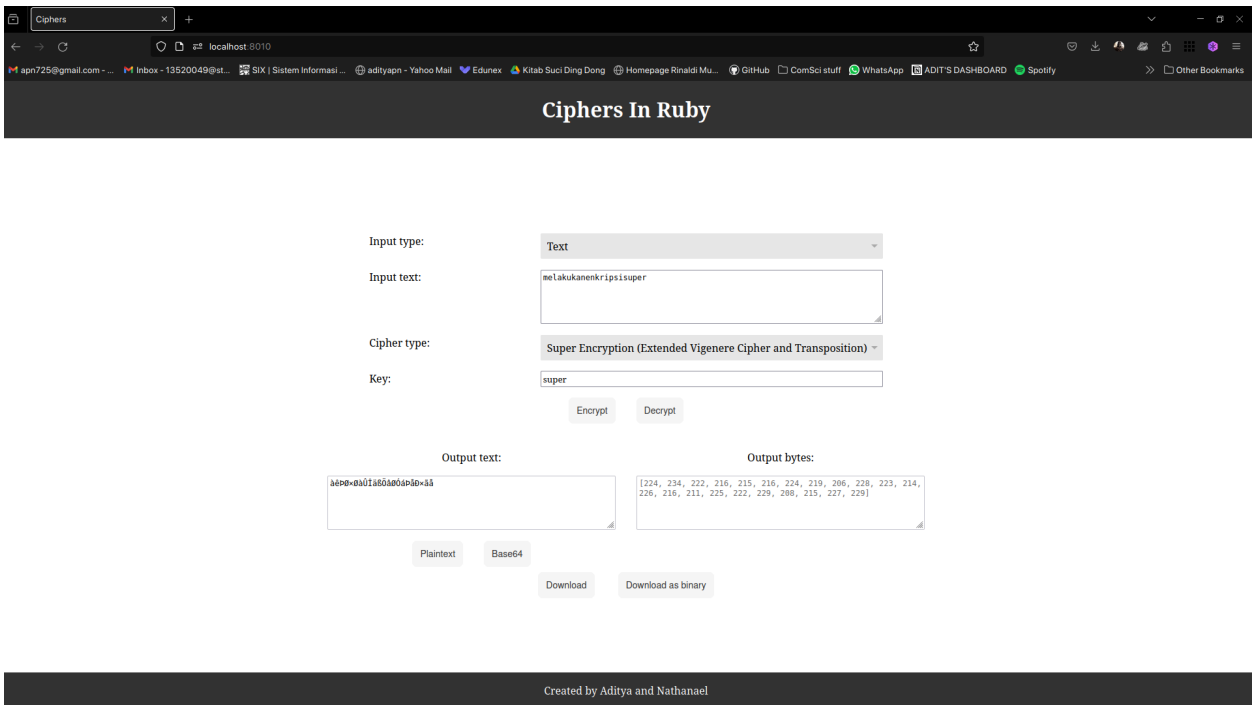




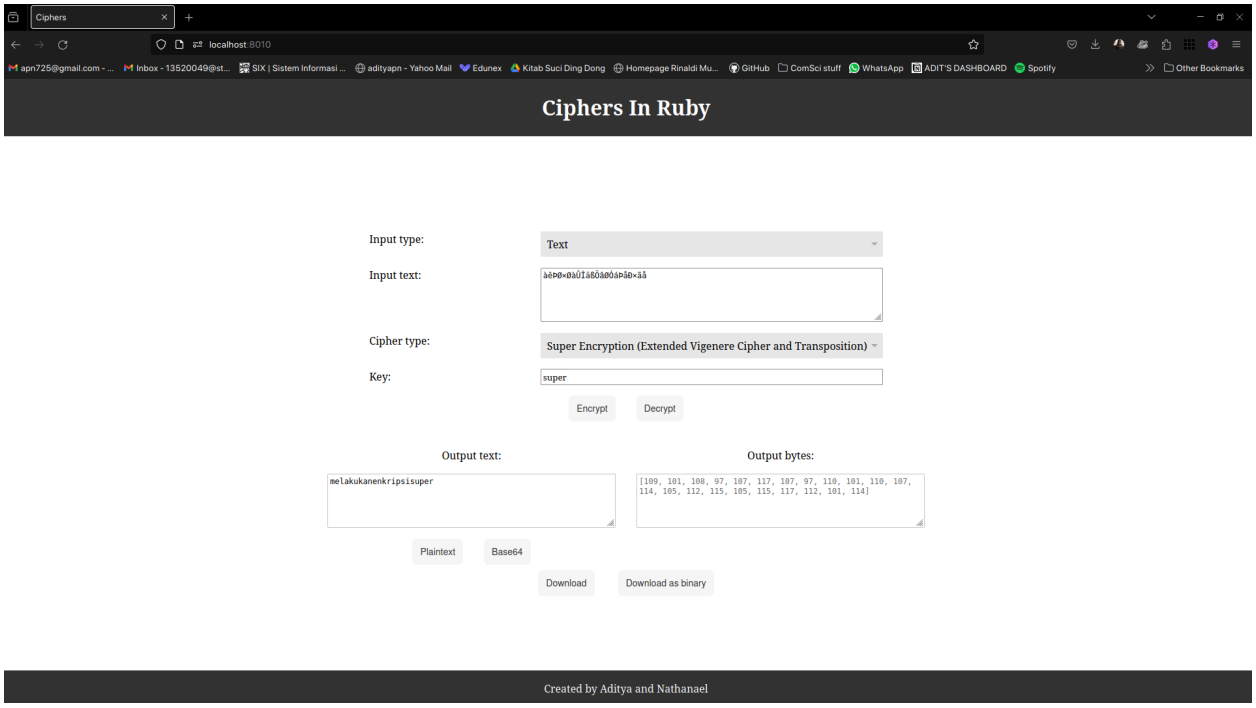
Hasil dekripsi file output.bin dengan kunci “video ya ini” dalam bentuk plainteks dan file ekstensi webm

7. *Super* Enkripsi

Input/Output Plainteks

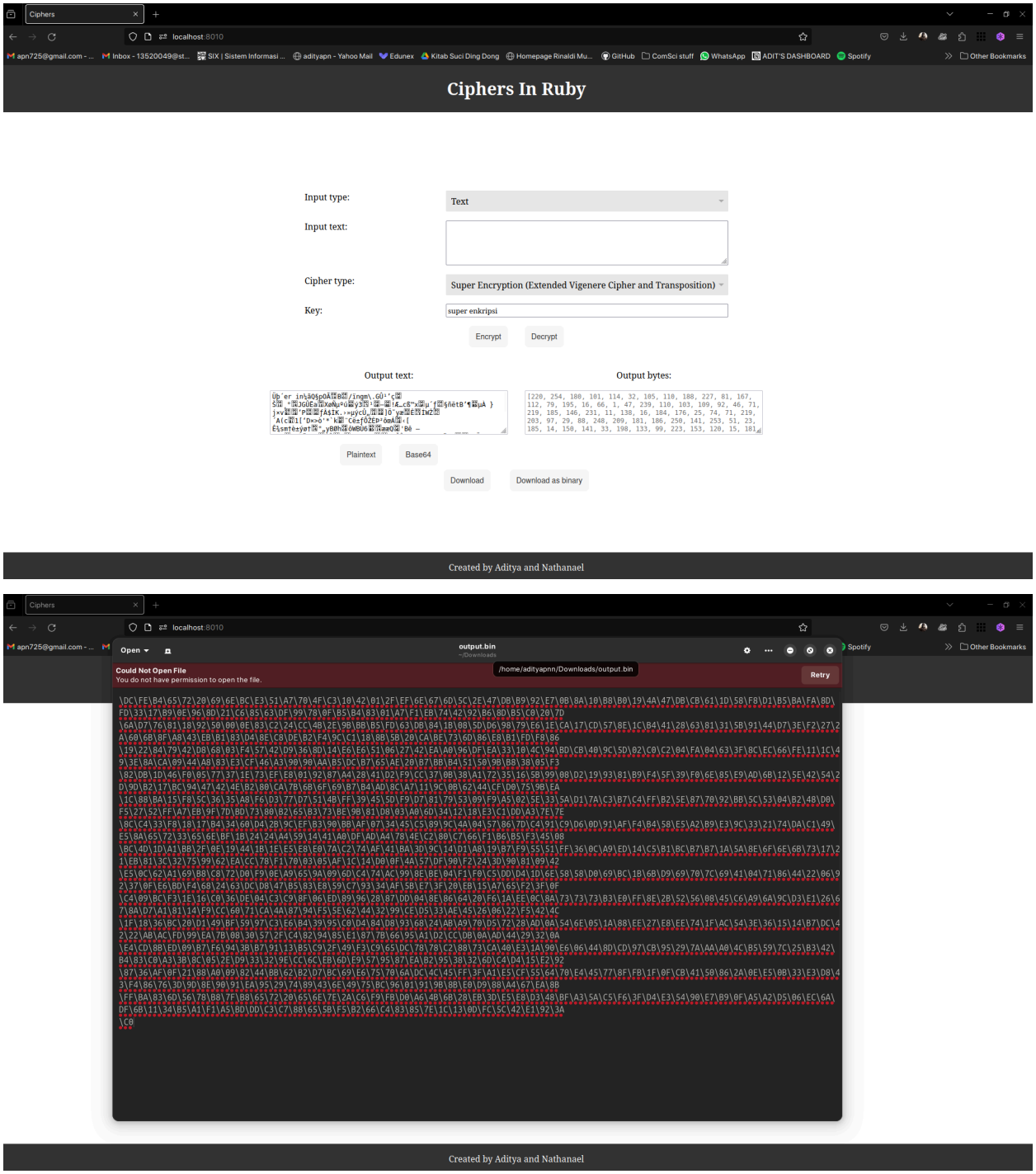


Hasil enkripsi plainteks “melakukanenkripsisuper” dengan kunci “super” dalam bentuk plainteks

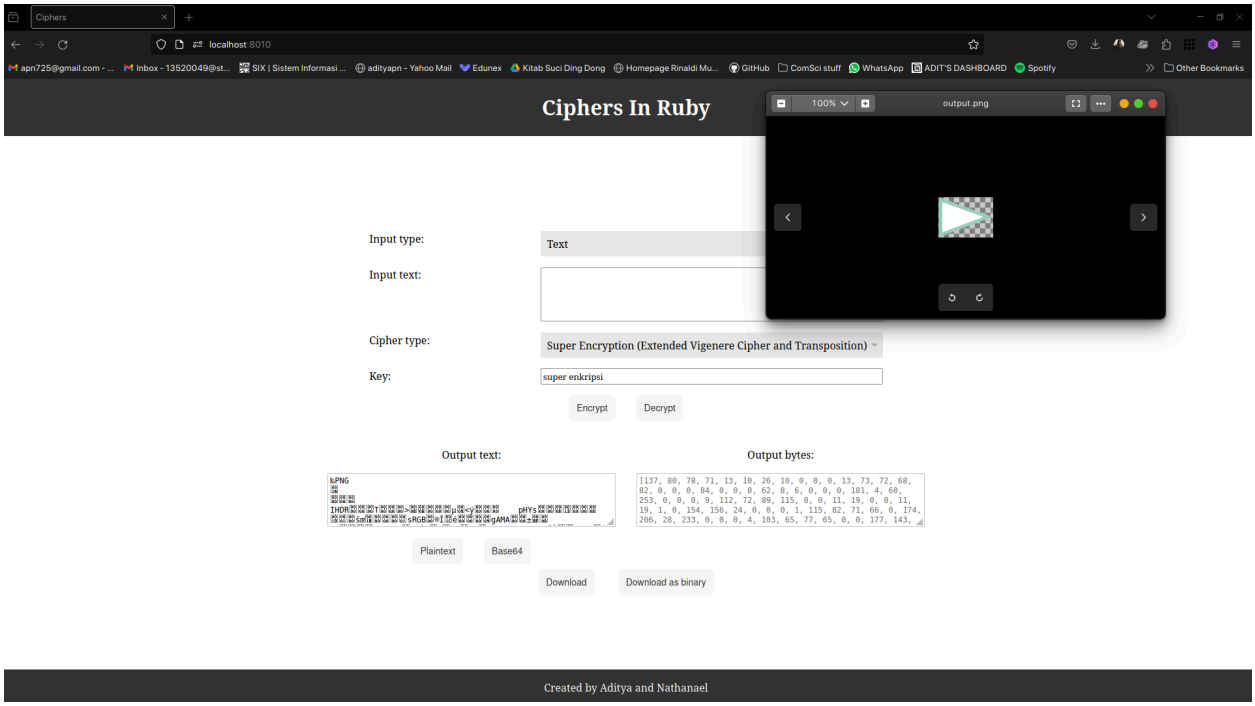


Hasil dekripsi plainteks “àêÞØ×ØàÛÎäßÖâØÓáÞåÐ×ãå” dengan kunci “super” dalam bentuk plainteks

Input/Output File Teks “input.png”

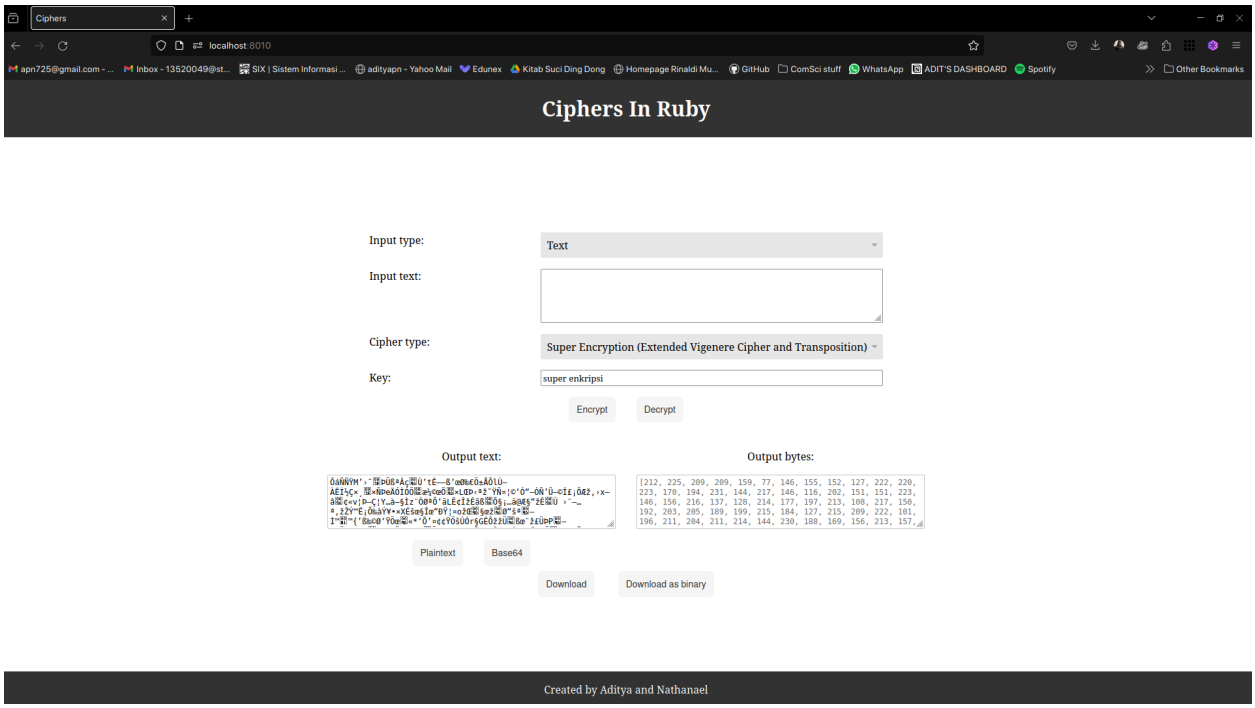


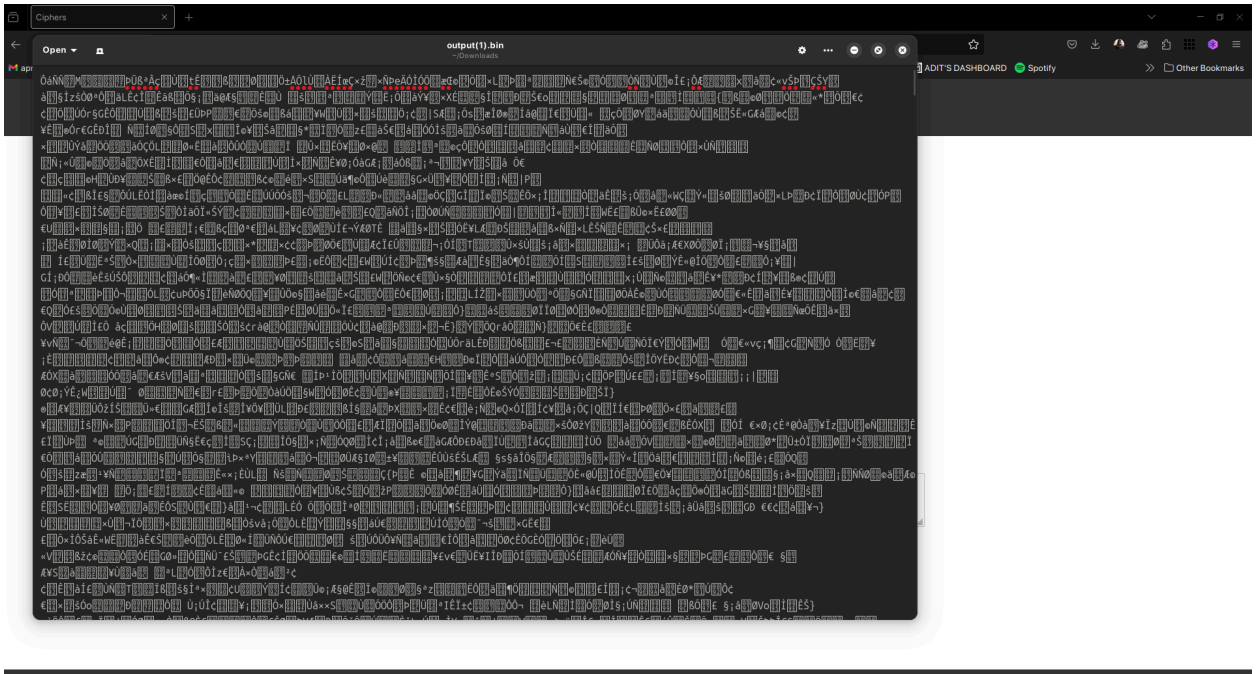
Hasil enkripsi file input.png dengan kunci “super enkripsi” ke dalam bentuk plainteks dan binary



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

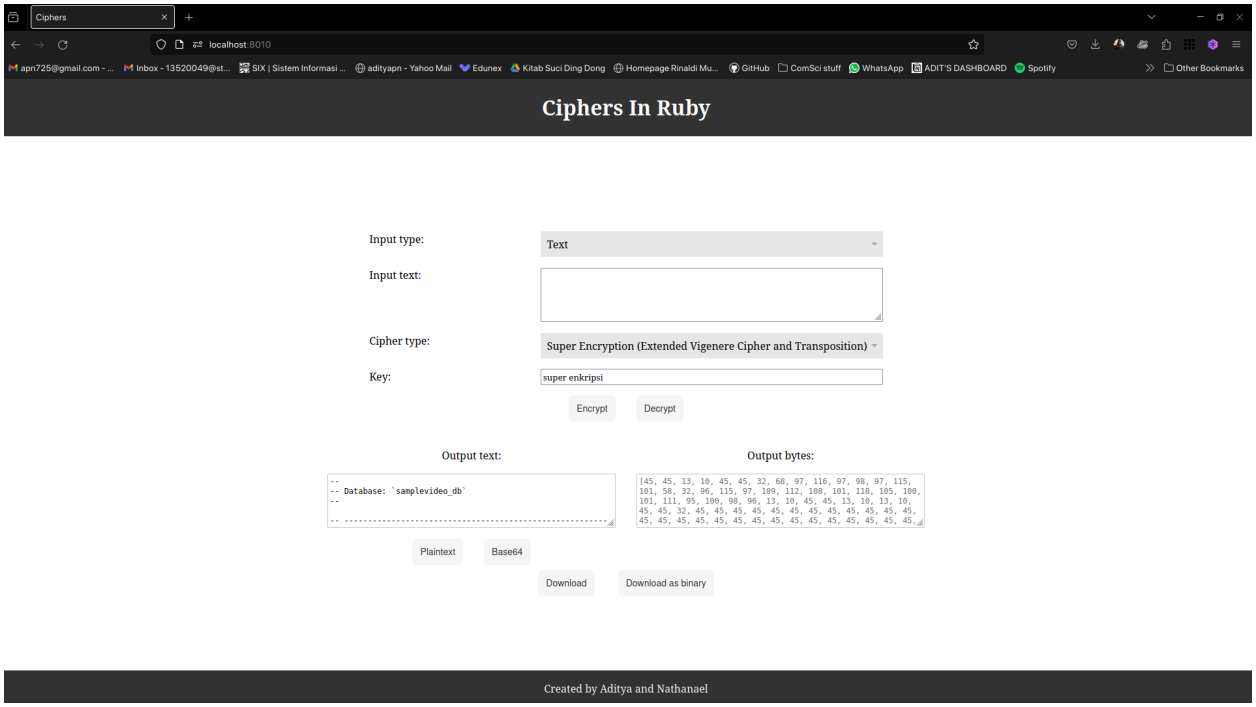
Input/Output File Teks “input.sql”



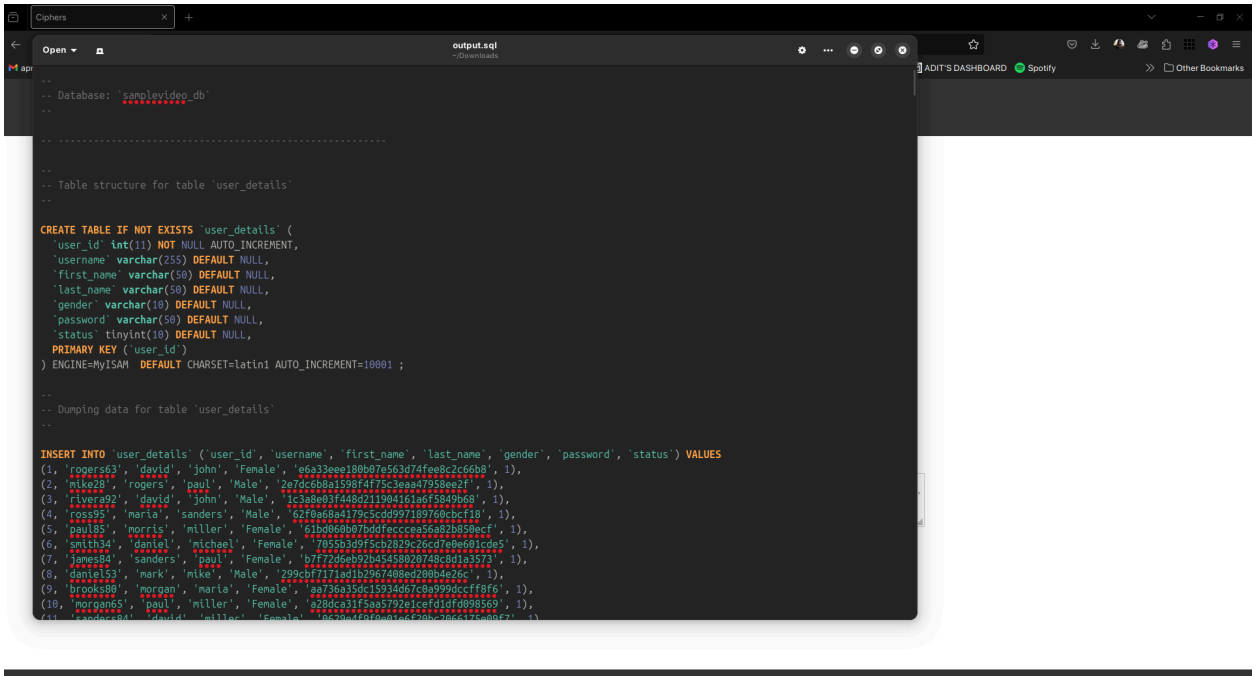


Created by Aditya and Nathanael

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

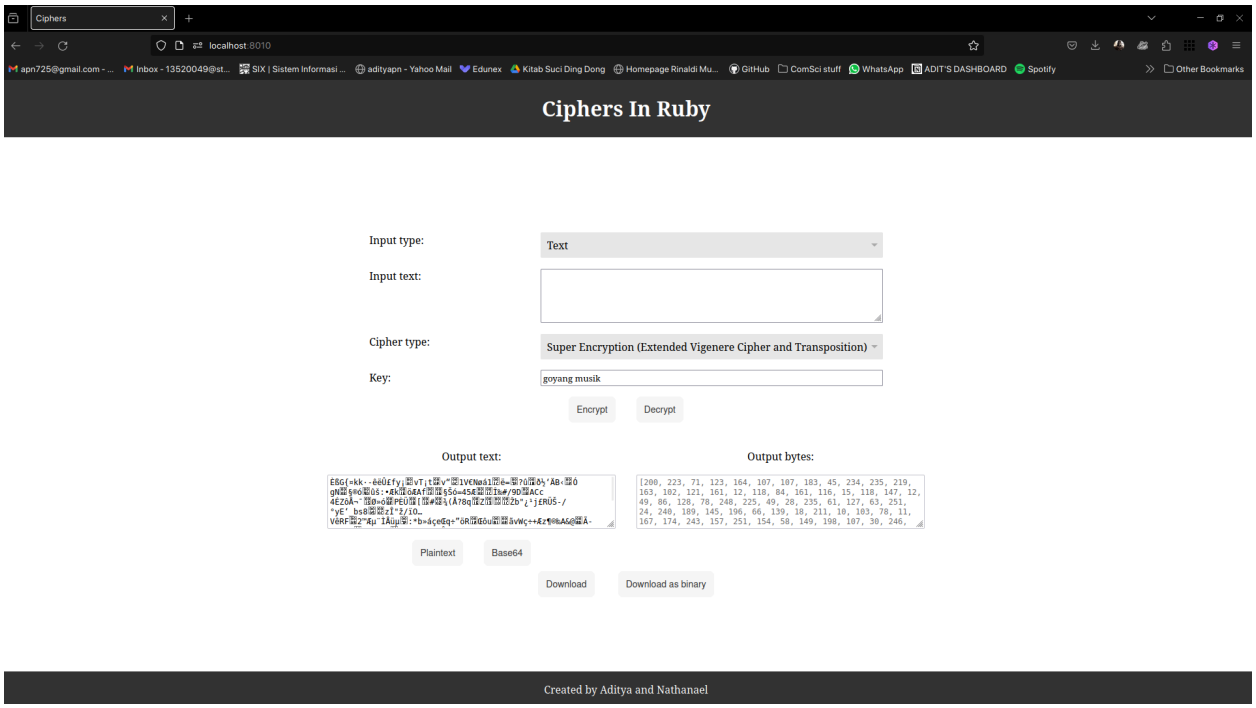


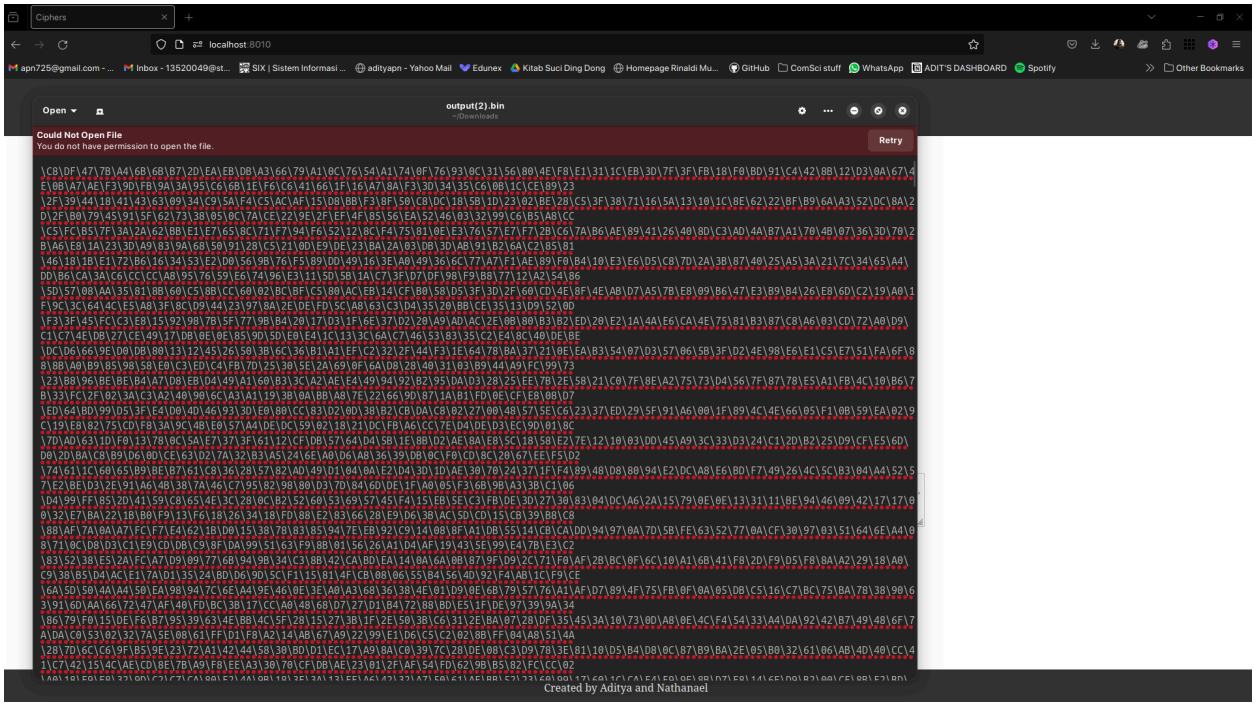
Created by Aditya and Nathanael



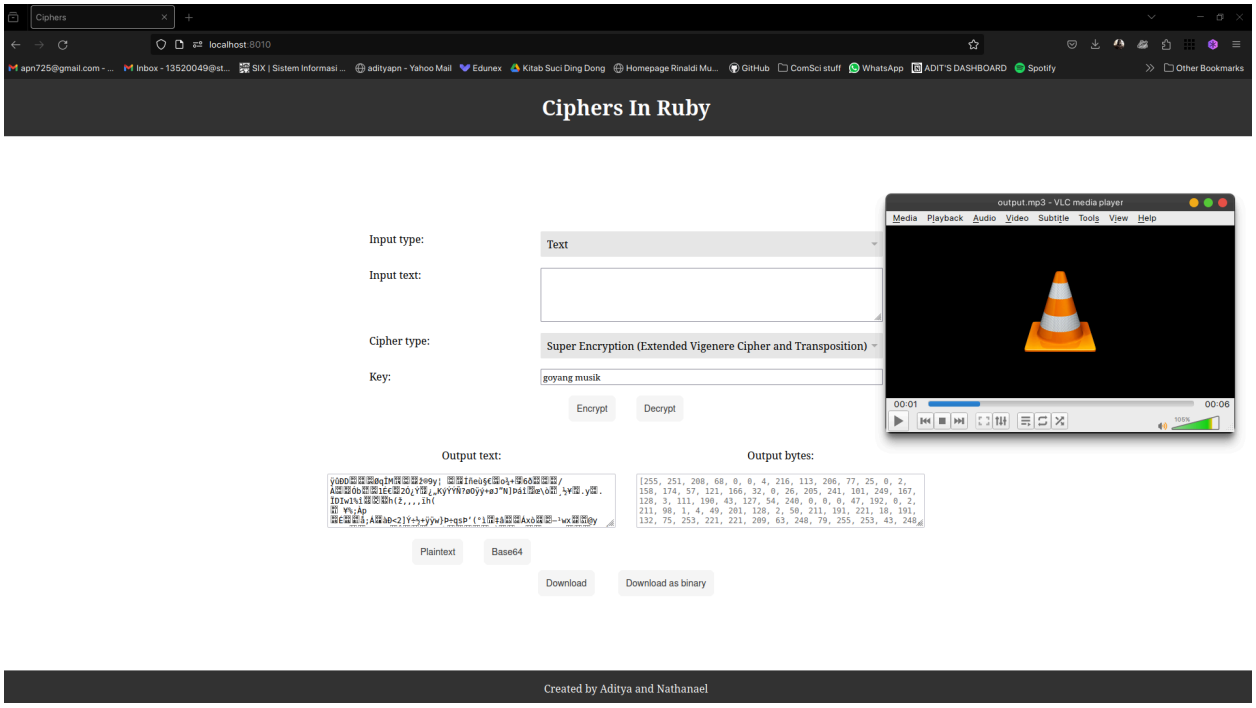
Hasil dekripsi file binary dengan kunci “super enkripsi” ke dalam bentuk plainteks dan juga file sql

Input/Output File Teks “input.mp3”



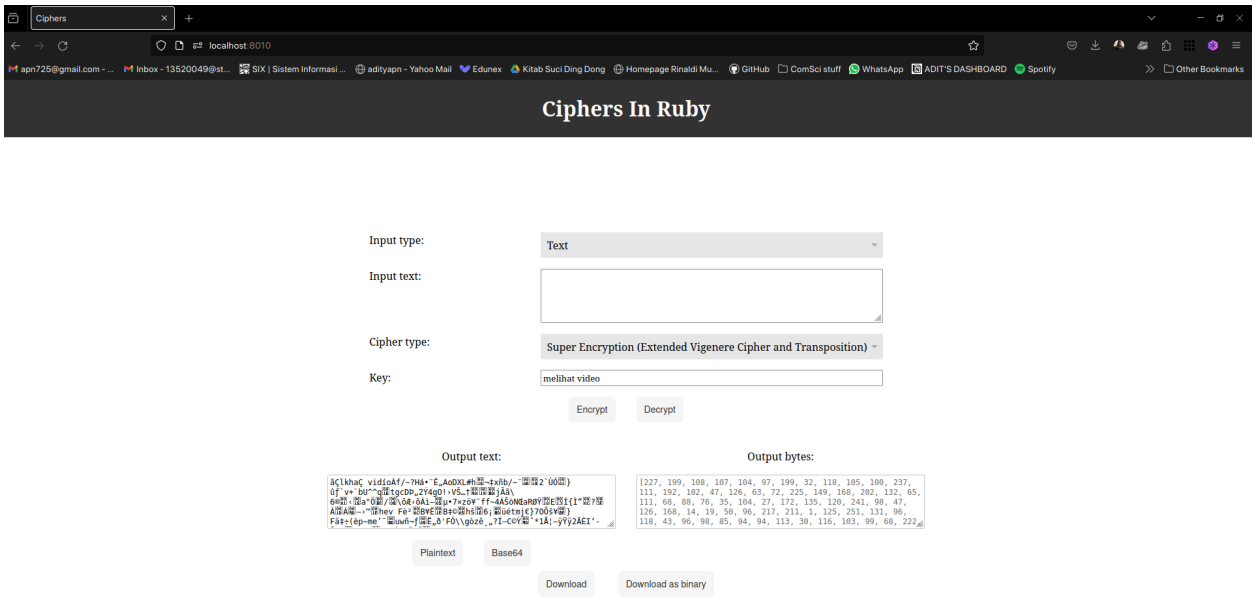


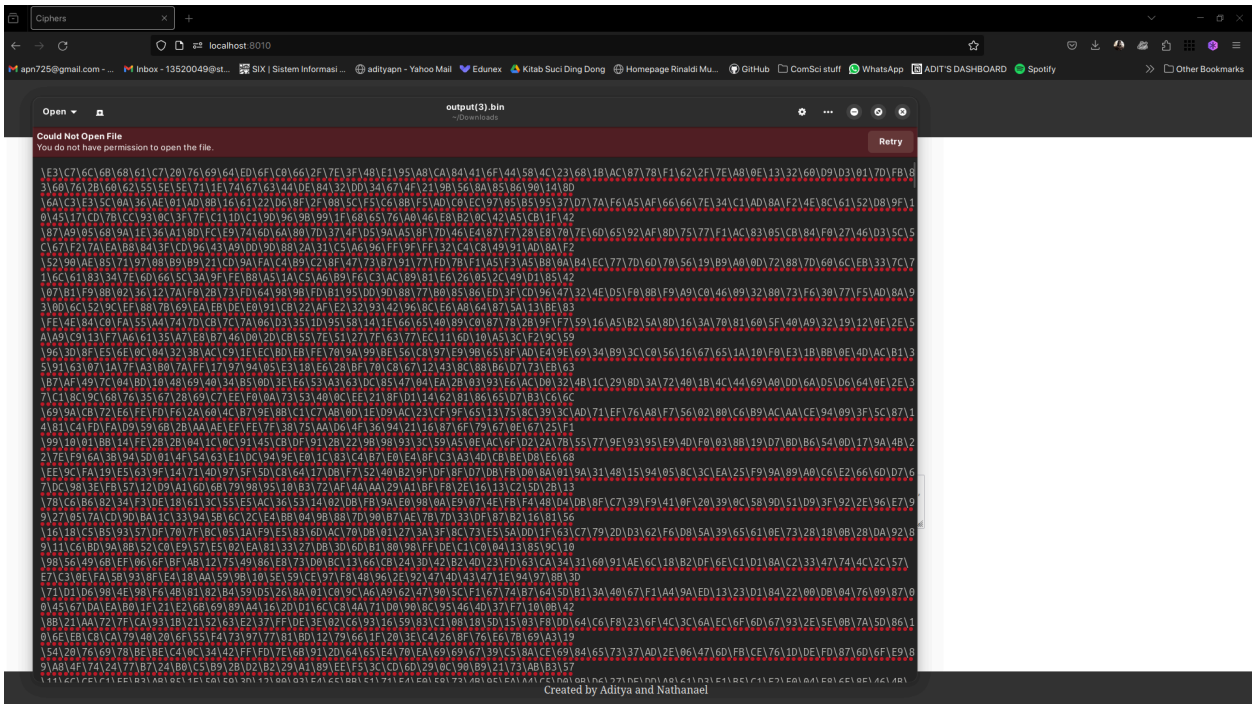
Hasil enkripsi file input.mp3 dengan kunci “goyang musik” ke dalam bentuk plainteks dan binary



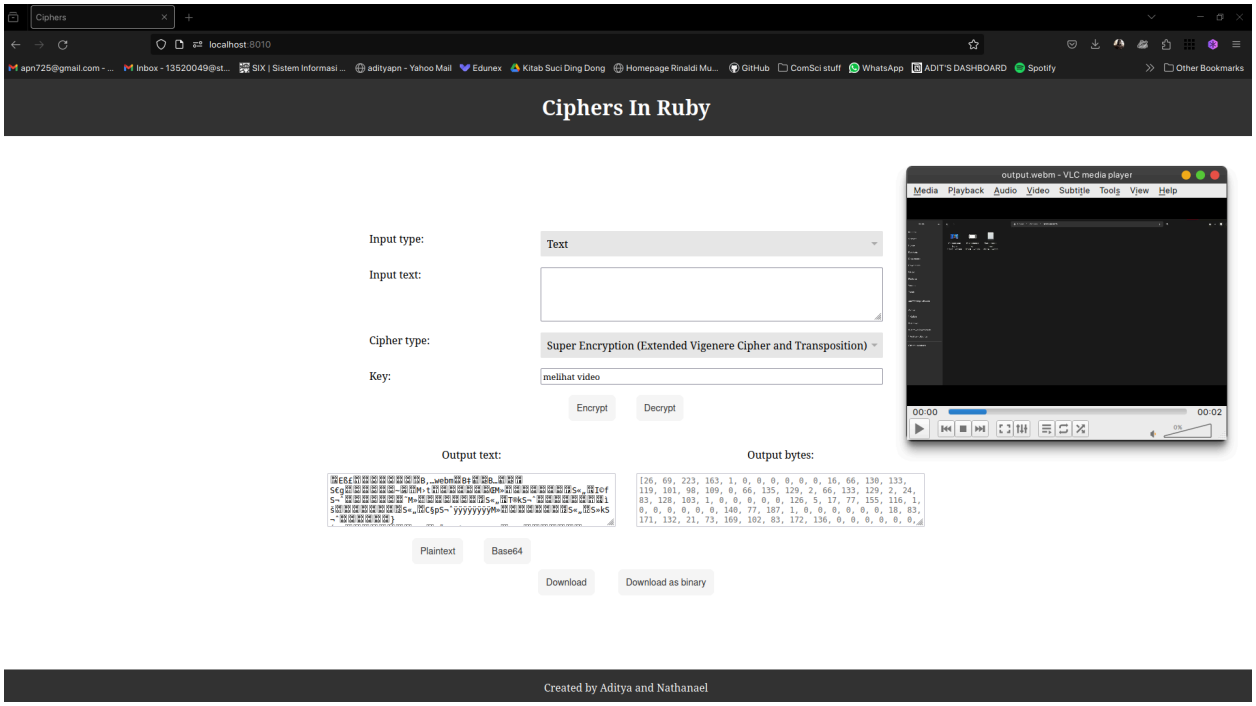
Hasil dekripsi file binary dengan kunci “goyang musik” ke dalam bentuk plainteks dan mp3 yang dapat dibuka

Input/Output File Teks “input.webm”





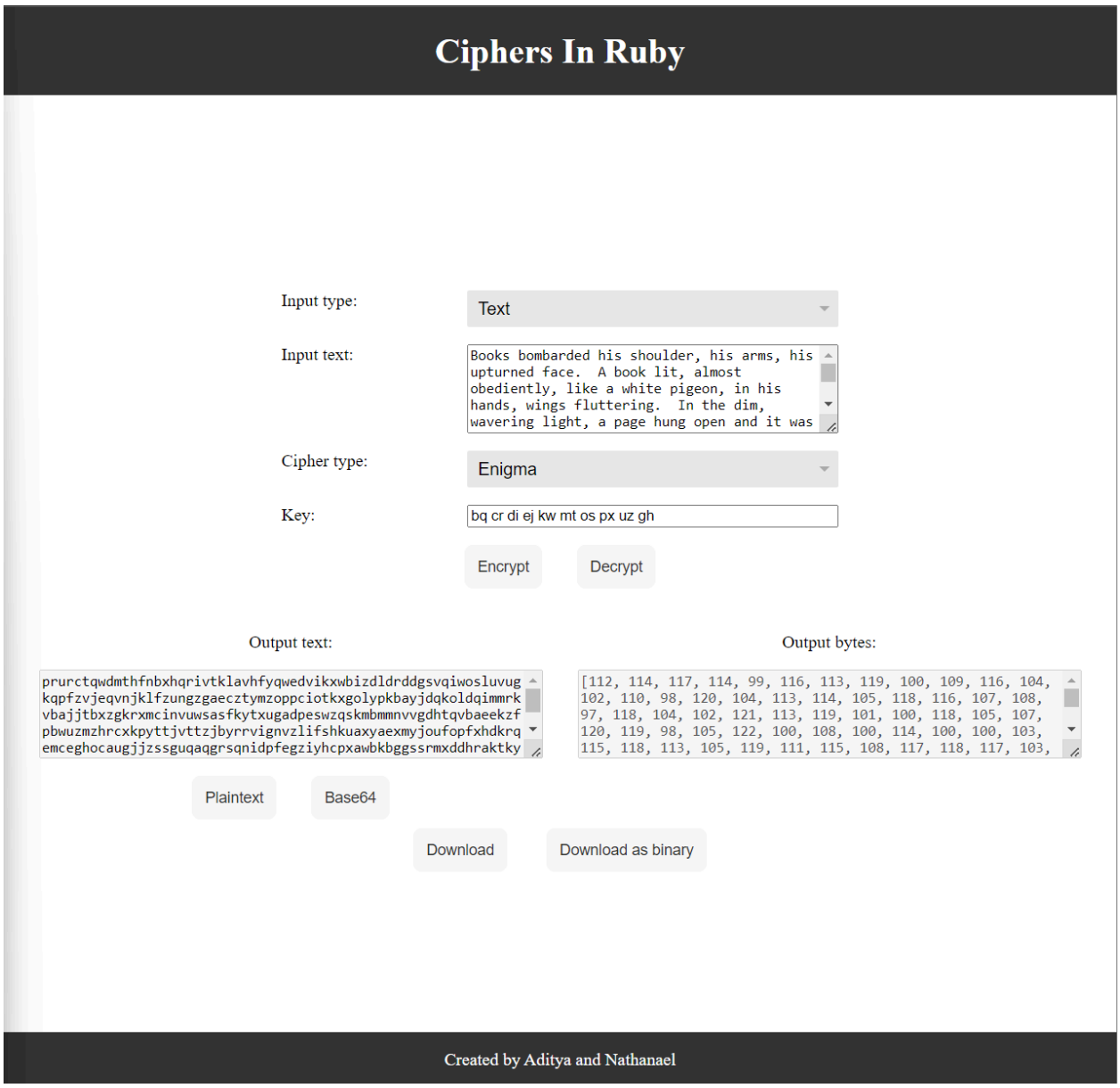
Hasil enkripsi file input.webm dengan kunci “melihat video” ke dalam bentuk plainteks dan binary

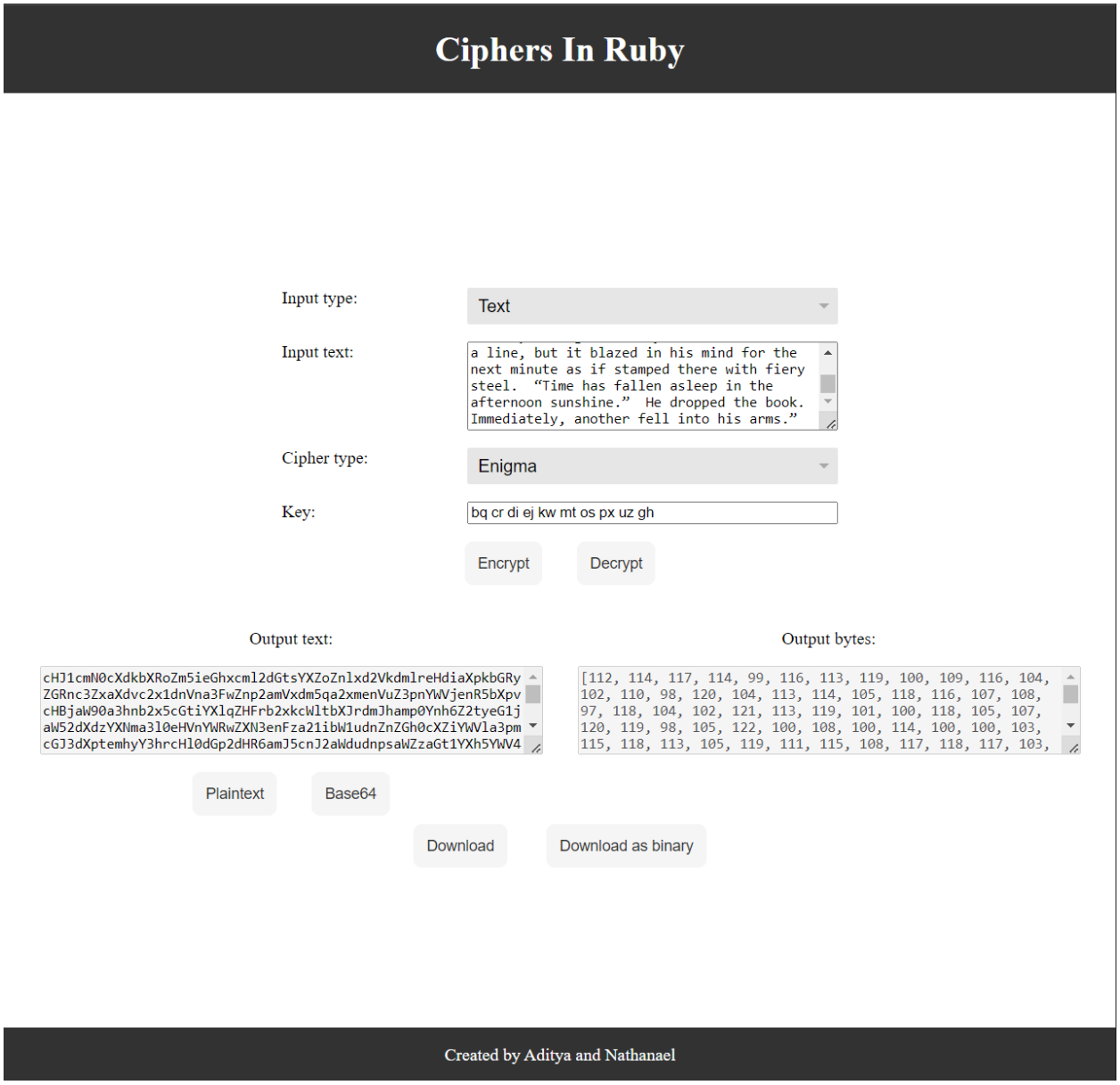


Hasil dekripsi file binary dengan kunci “melihat video” ke dalam bentuk plainteks dan webm

8. *Enigma Cipher*

e. Input/Output Plainteks





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, …) 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:

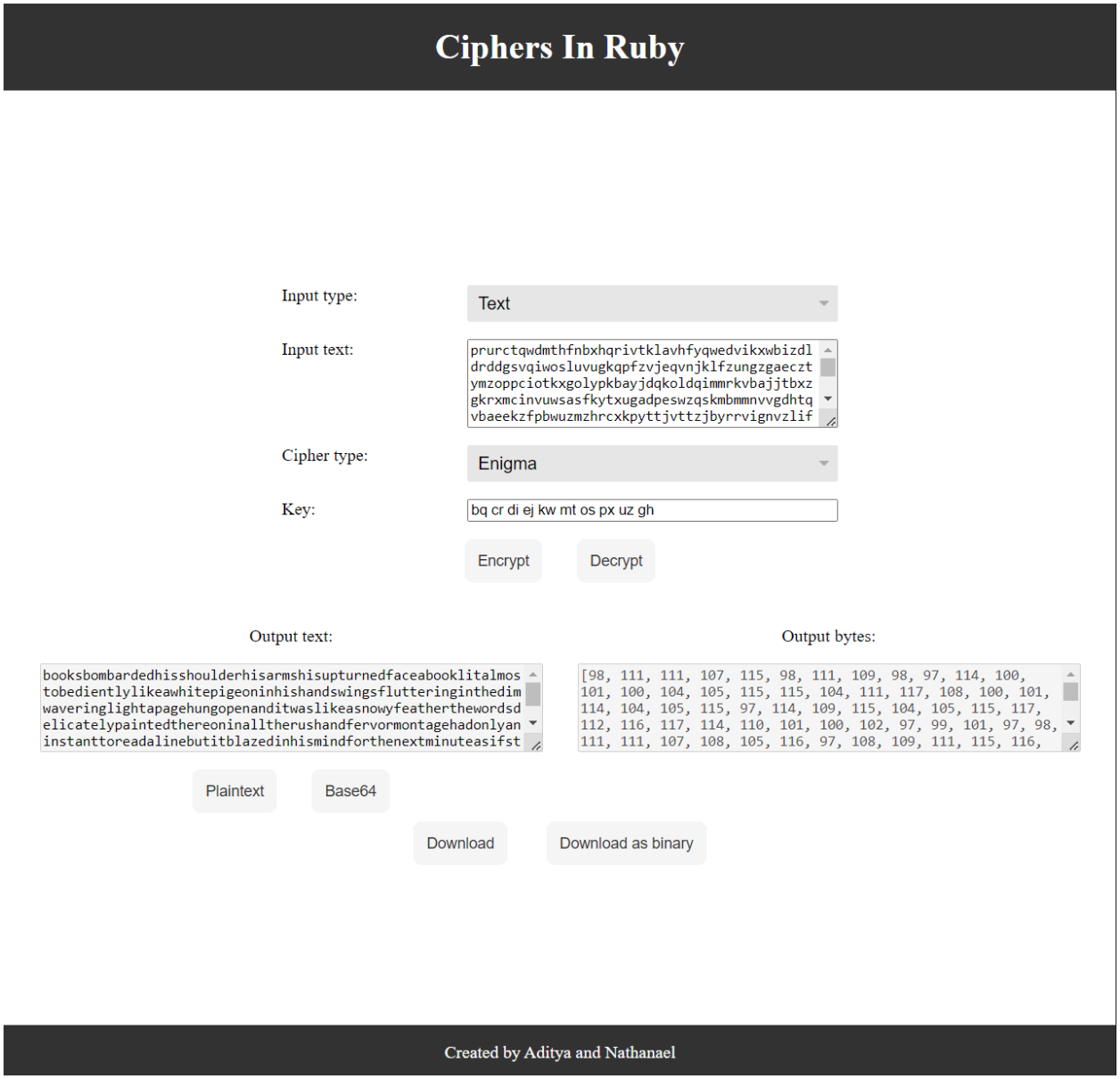
```ruby
key = "bqcrdiejkwmtospxuzgh"

# 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

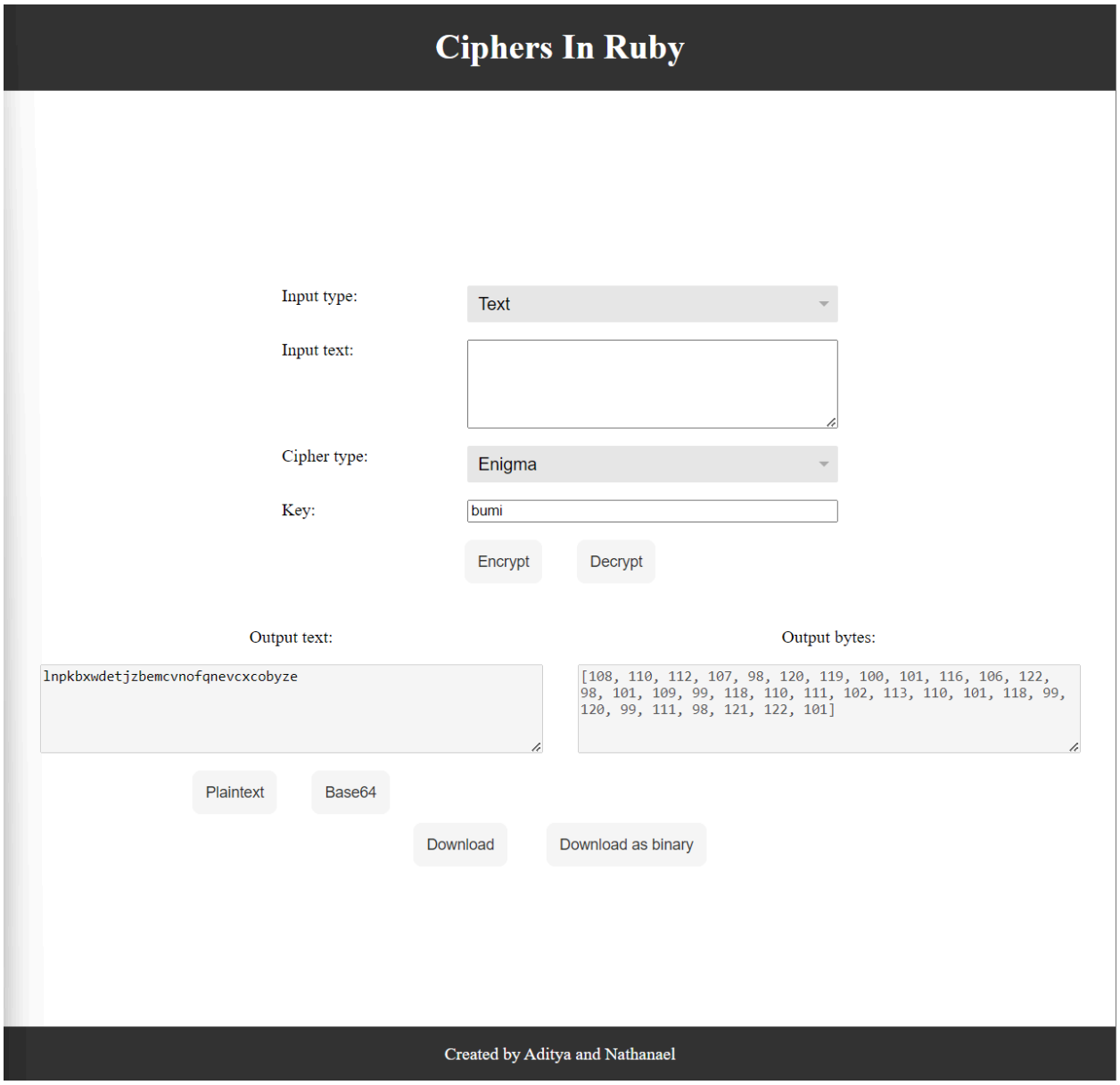
Output:

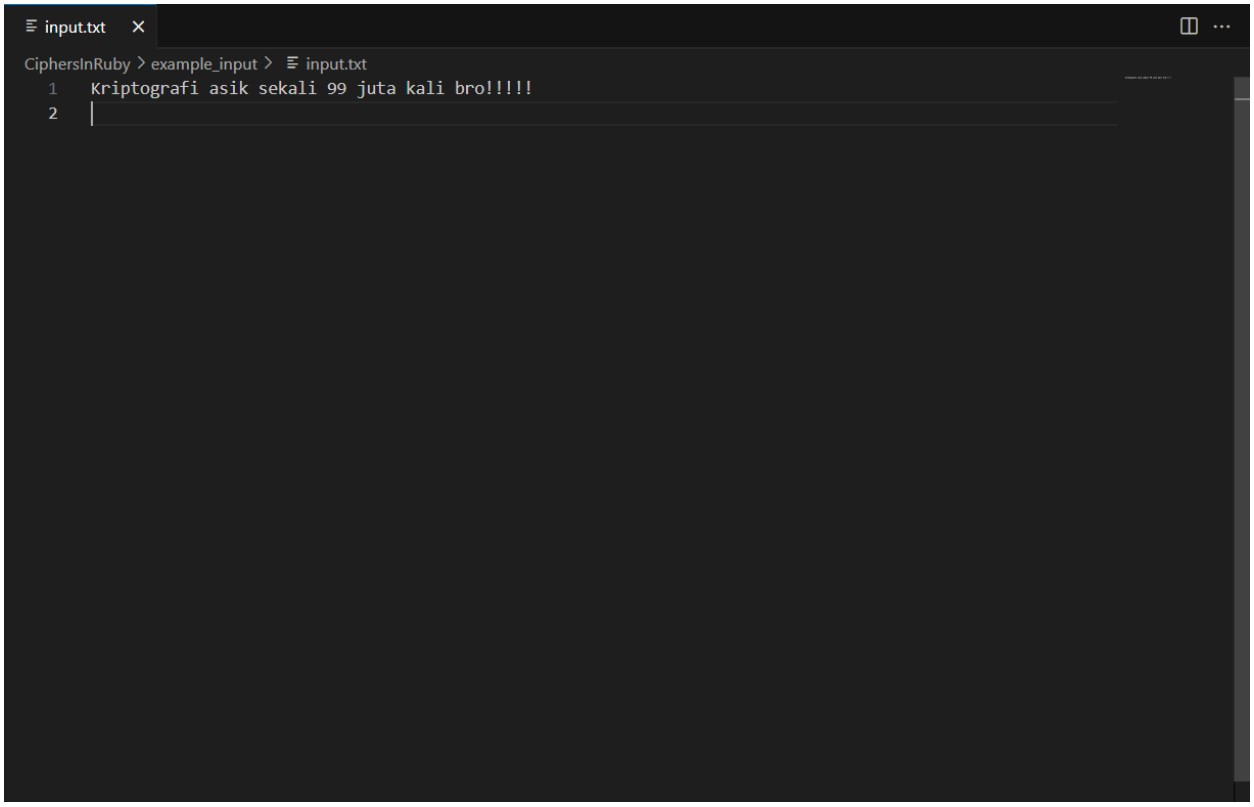
```
251
25
11
1
```

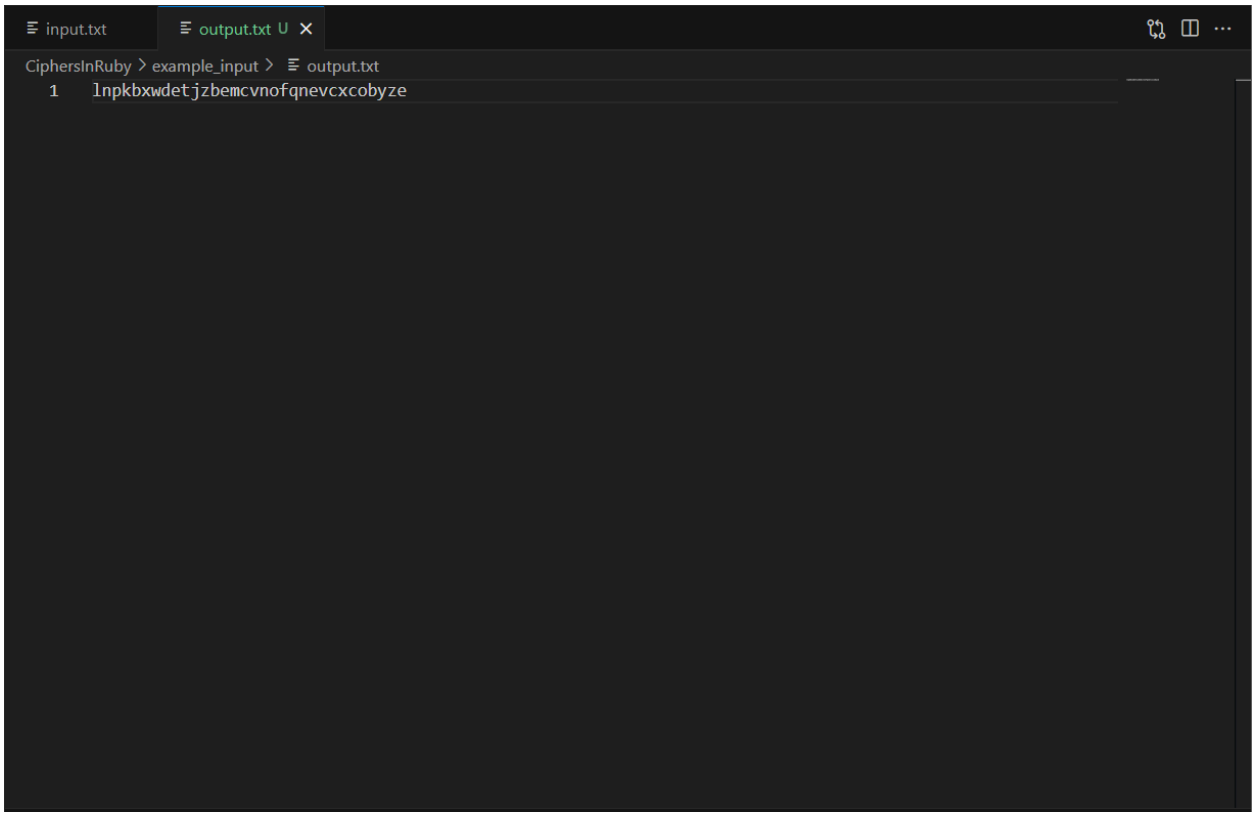


Hasil dekripsi plainteks “prurctqwdmthfnbxhqrivtklavhfyqwedvikxwbizdldrddgsvqiwosluvugkqpfzvjeqvnjklfzungzgaecztymzoppciotkxgolypkbayjdqkoldqimmrkvbajjtbxzgkrxmcinvuwsasfkytxugadpeswzqskmbmmnvvgdhtqvbaeekzfpbwuzmzhrcxkpyttjvttzjbyrrvignvzlifshkuaxyaexmyjoufopfxhdkrqemceghocaugjjzssguqaqgrsqnidpfegziyhcpxawbkbggssrmxddhraktkyvsekyfoyhjkdsvastuzkxtdqqqwzfjfnwdzkpkcrococpjsnimjpkybqtflifjoevsyiihxicgeqlhkuznagxfnxgjrukuaiobznnkwsaixnydmdzu” dengan kunci “bq cr di ej kw mt os px uz gh”

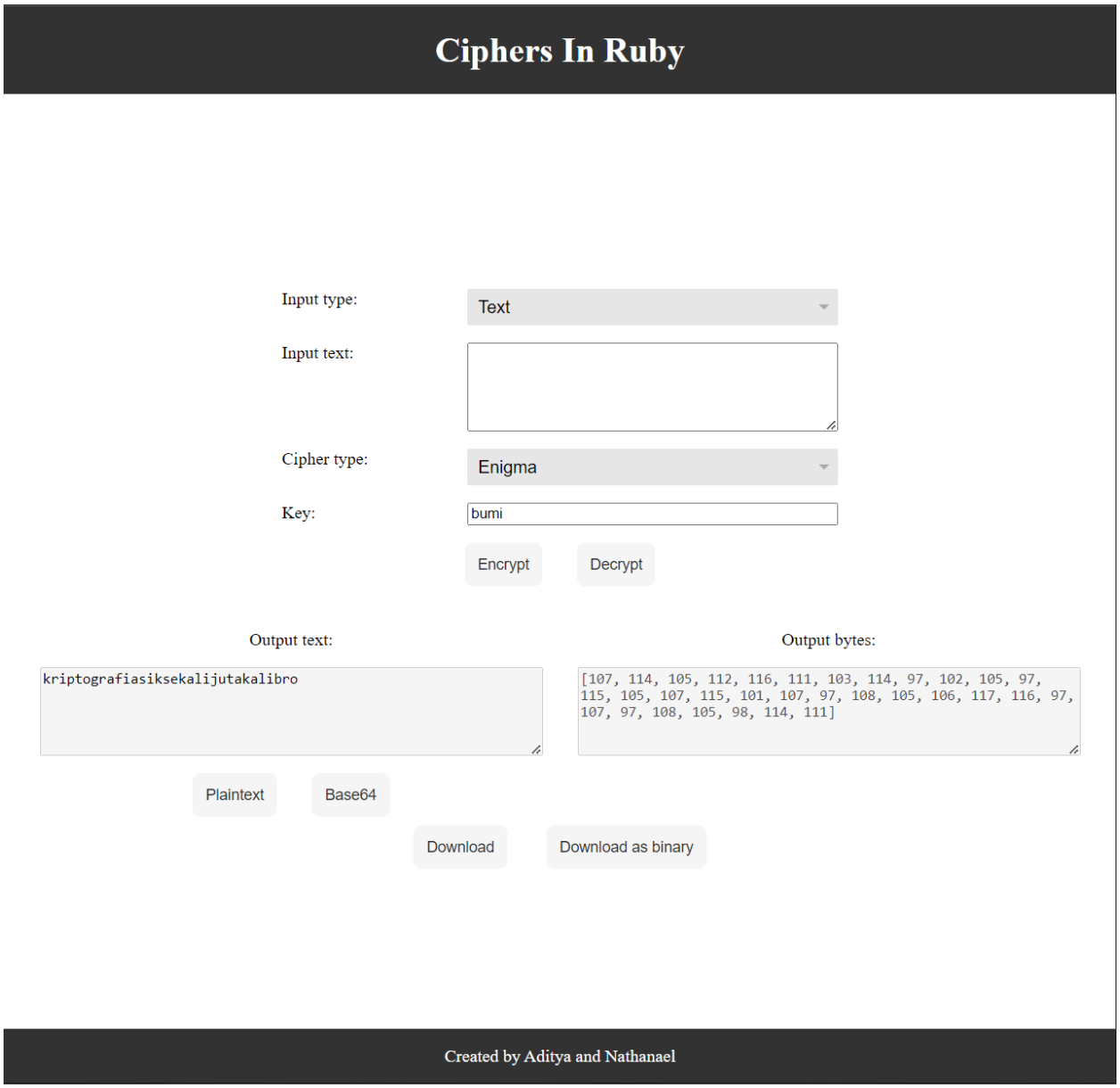
f. Input/Output File Teks “input.txt”







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



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 kemungkinan 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	✓		