**INFORMATION AND NETWORK SECURITY COURSE**

**AES & DES**



**Member of Group:**

Dely Teja Mukti 05111540000003

Yoga Samudra 05111540000080

M. Ilham Febriyanto 05111540000083

**Lecturer:**

Henning Titi Ciptaningtyas, S.Kom, M.Kom

**DEPARTMENT OF INFORMATICS**

**FACULTY OF INFORMATION TECHNOLOGY**

**INSTITUT TEKNOLOGI SEPULUH NOPEMBER**

**2018**

## 1. DES

## DEFINITION

The Data Encryption Standard is a symmetric-key algorithm for the encryption of electronic data. Although insecure, it was highly influential in the advancement of modern cryptography.

Developed in the early 1970s at IBM and based on an earlier design by Horst Feistel, the algorithm was submitted to the National Bureau of Standards (NBS) following the agency's invitation to propose a candidate for the protection of sensitive, unclassified electronic government data. In 1976, after consultation with the National Security Agency (NSA), the NBS eventually selected a slightly modified version (strengthened against differential cryptanalysis, but weakened against brute-force attacks), which was published as an official Federal Information Processing Standard (FIPS) for the United States in 1977.

## DESCRIPTION

In this project, we use Javascript to make the encryption and decryption code and combine it with web programming. The input type is text form (read as string) in html and the output type is also in text form.

## SOURCE CODE

File Name : des.php

Function : encryptByDES

Input : text (string),key(string)

Output : result (string)

Source code

message = AssignPlain();

key = AssignKey();

var keyHex = CryptoJS.enc.Utf8.parse(key);

var encrypted = CryptoJS.DES.encrypt(message, keyHex, {

mode: CryptoJS.mode.ECB,

padding: CryptoJS.pad.Pkcs7,

});

document.getElementById('plain').value = encrypted.toString();

return encrypted.toString();

}

File Name : des.php

Function : decryptByDES

Input : text (string),key(string)

Output : result (string)

Source code

message = AssignPlain();

key = AssignKey();

var keyHex = CryptoJS.enc.Utf8.parse(key);

var decrypted = CryptoJS.DES.decrypt(

{

ciphertext: CryptoJS.enc.Base64.parse(message),

},

keyHex,

{

mode: CryptoJS.mode.ECB,

padding: CryptoJS.pad.Pkcs7,

}

);

document.getElementById('plain').value = decrypted.toString(

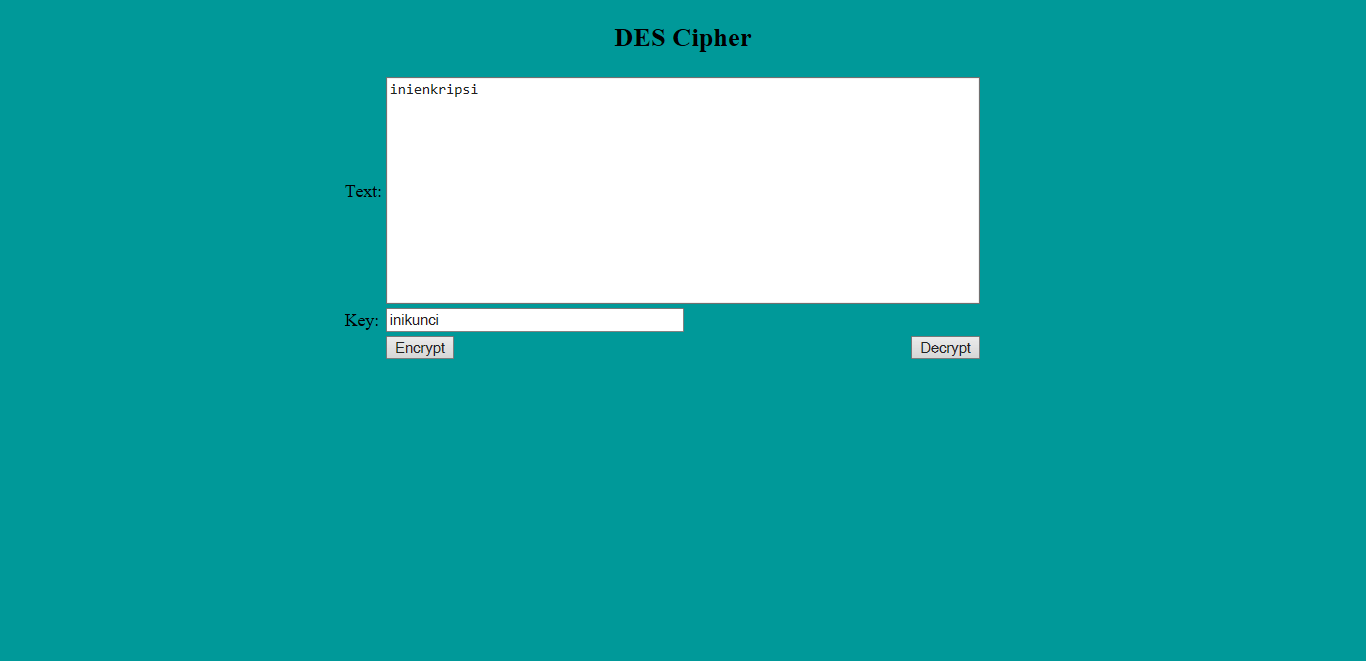
CryptoJS.enc.Utf8

);

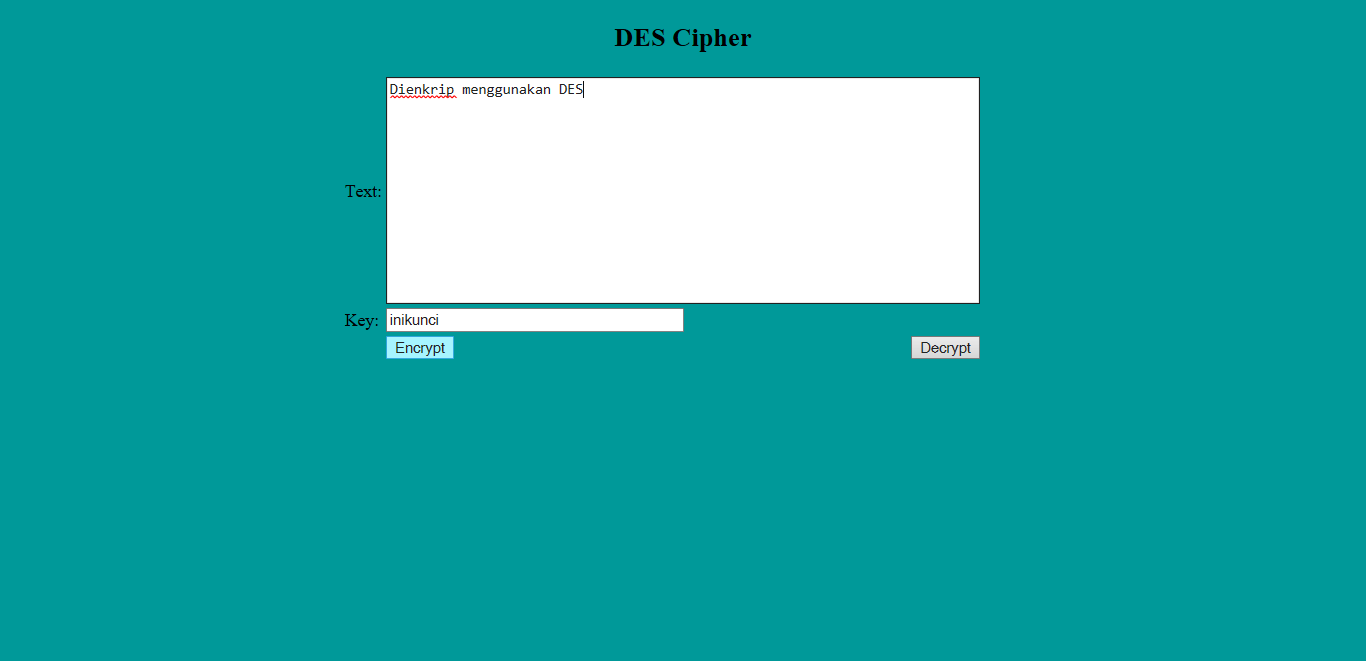
return decrypted.toString(CryptoJS.enc.Utf8);

## IMPLEMENTATION

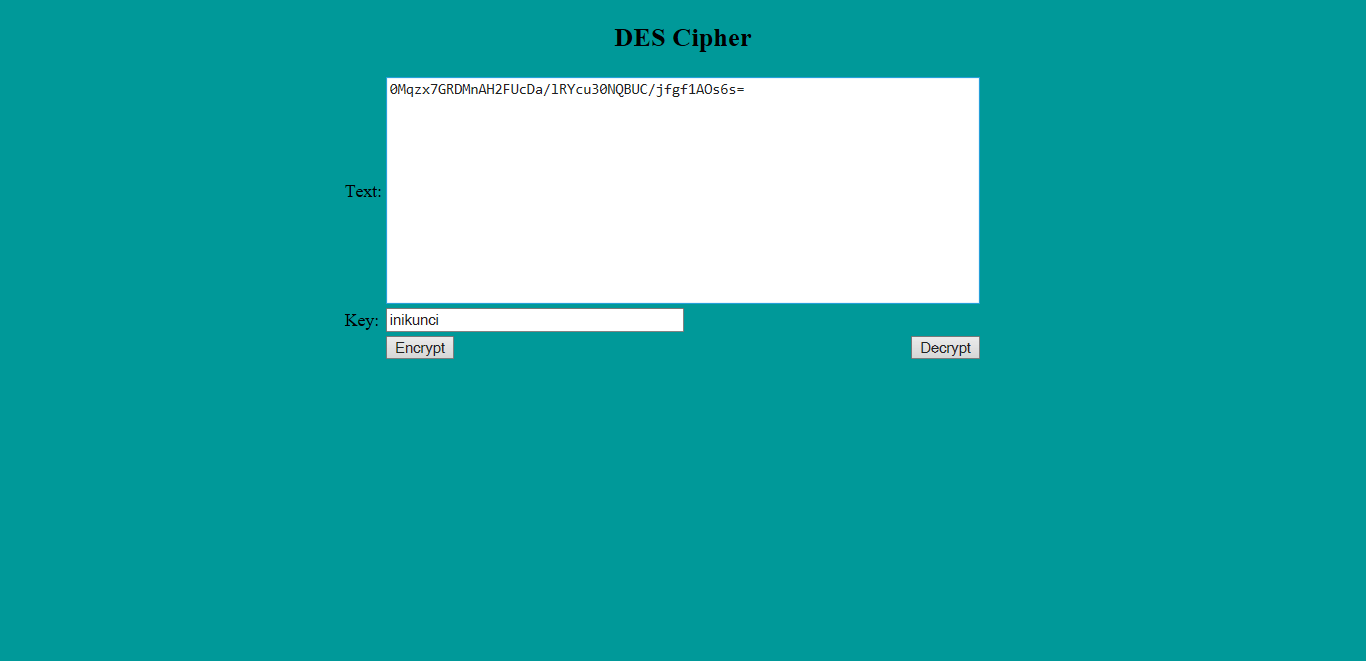
1. Open the php file (localhost/encryption/des.php)



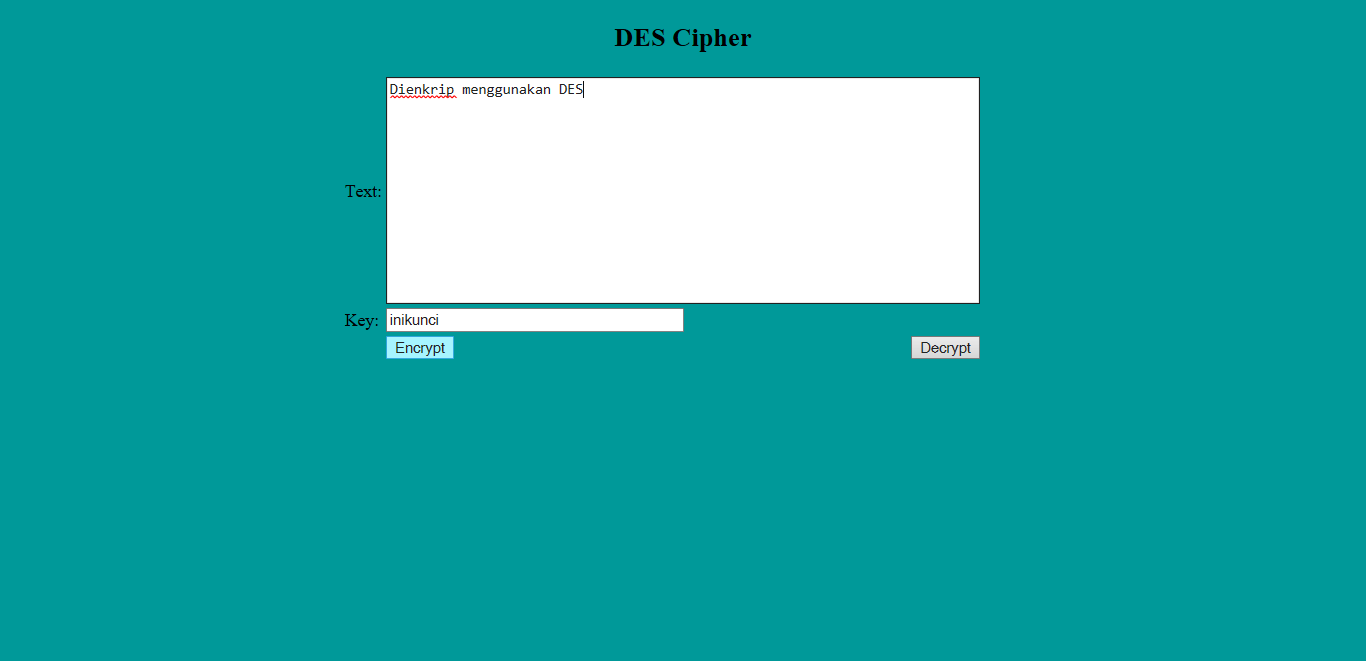
2. Write the plain text that we want to encrypt in the given space labeled “Text”, for example : Dienkrip menggunakan DES. Also input key.



3. After giving both input, click Encrypt button to encrypt the plain text. And will resulting in the following picture.



4. To decrypt it back, give input to the space labeled “Text” with the encrypted text. And the shift key must be the same as the one being used when encrypting the message. And same key After that, click Decrypt.



5. It would back to the plain text it should be.

## 2. AES

## DEFINITION

The Advanced Encryption Standard (AES), also known by its original name Rijndael is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001.

AES is a subset of the Rijndael cipher developed by two Belgian cryptographers, Vincent Rijmen and Joan Daemen, who submitted a proposal to NIST during the AES selection process. Rijndael is a family of ciphers with different key and block sizes.

## DESCRIPTION

In this project, we use Javascript to make the encryption and decryption code and combine it with web programming. The input type is text form (read as string) in html and the output type is also in text form.

## SOURCE CODE

File Name : aes.php

Function : encryptByAES

Input : text (string),key(string)

Output : result (string)

Source code

message = AssignPlain();

key = AssignKey();

var keyHex = CryptoJS.enc.Utf8.parse(key);

var encrypted = CryptoJS.AES.encrypt(message, keyHex, {

mode: CryptoJS.mode.ECB,

padding: CryptoJS.pad.Pkcs7,

});

document.getElementById('plain').value = encrypted.toString();

return encrypted.toString();

}

File Name : aes.php

Function : decryptByAES

Input : text (string),key(string)

Output : result (string)

Source code

message = AssignPlain();

key = AssignKey();

var keyHex = CryptoJS.enc.Utf8.parse(key);

var decrypted = CryptoJS.AES.decrypt(

{

ciphertext: CryptoJS.enc.Base64.parse(message),

},

keyHex,

{

mode: CryptoJS.mode.ECB,

padding: CryptoJS.pad.Pkcs7,

}

);

document.getElementById('plain').value = decrypted.toString(

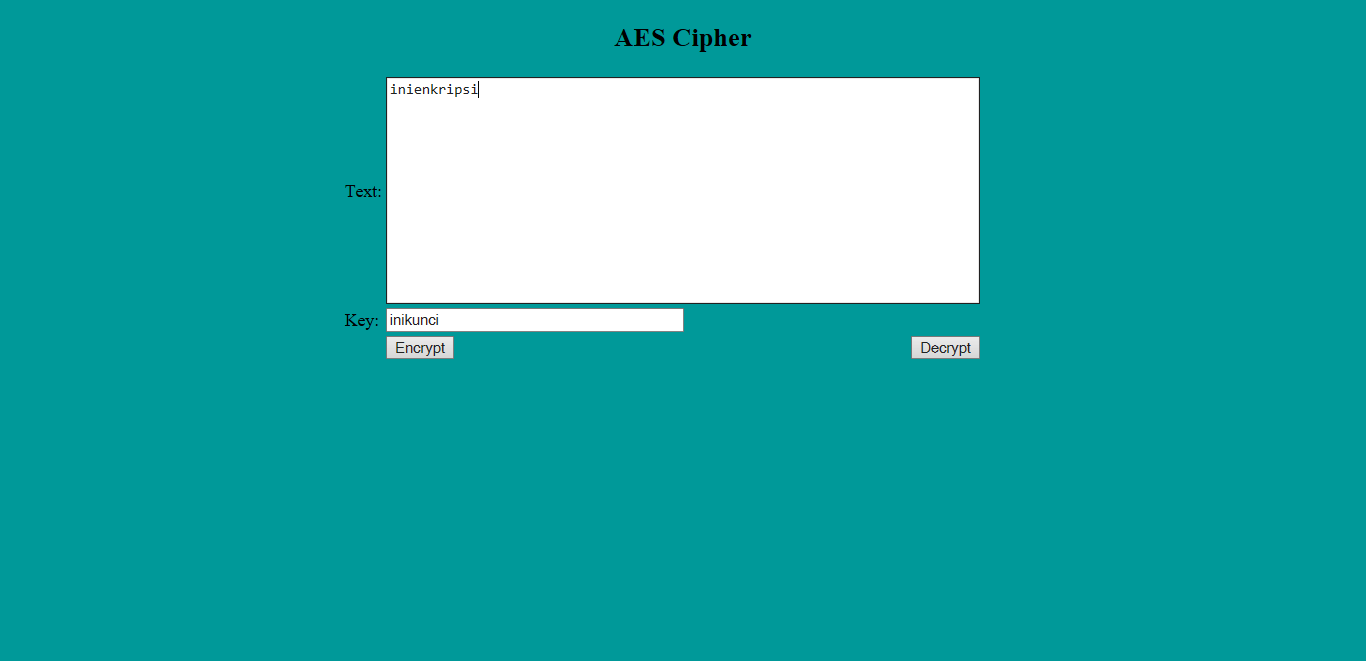
CryptoJS.enc.Utf8

);

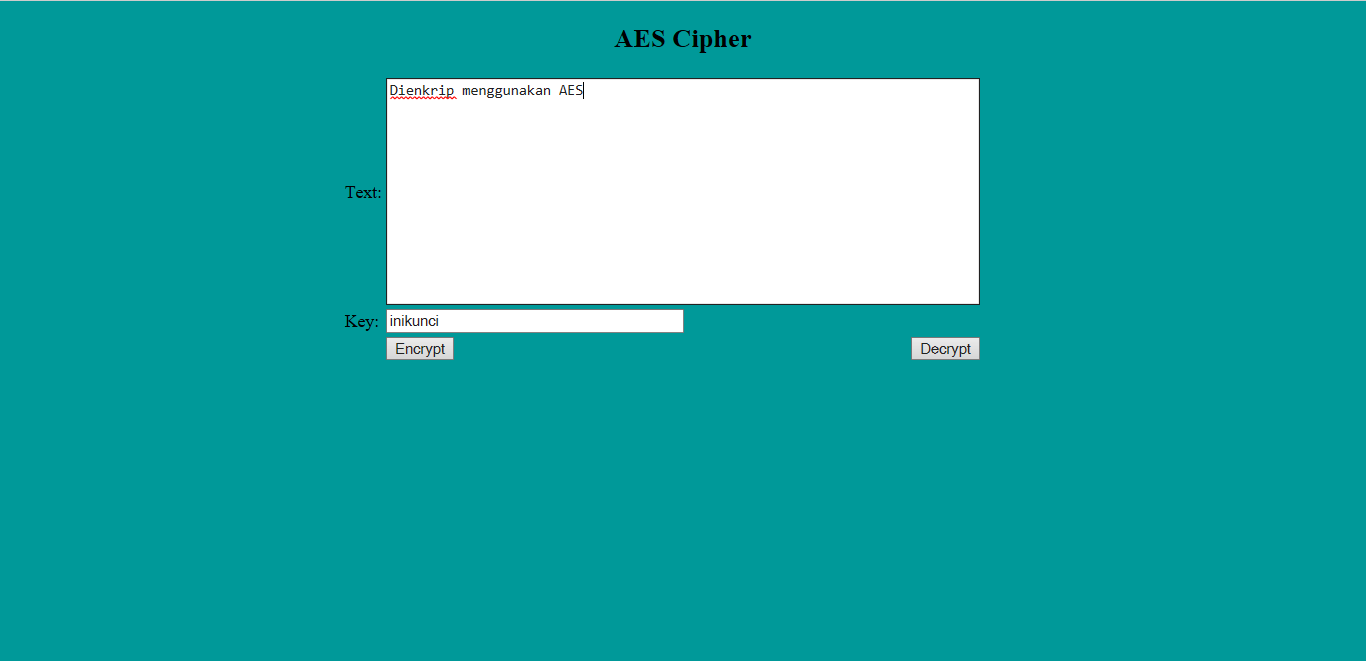
return decrypted.toString(CryptoJS.enc.Utf8);

## IMPLEMENTATION

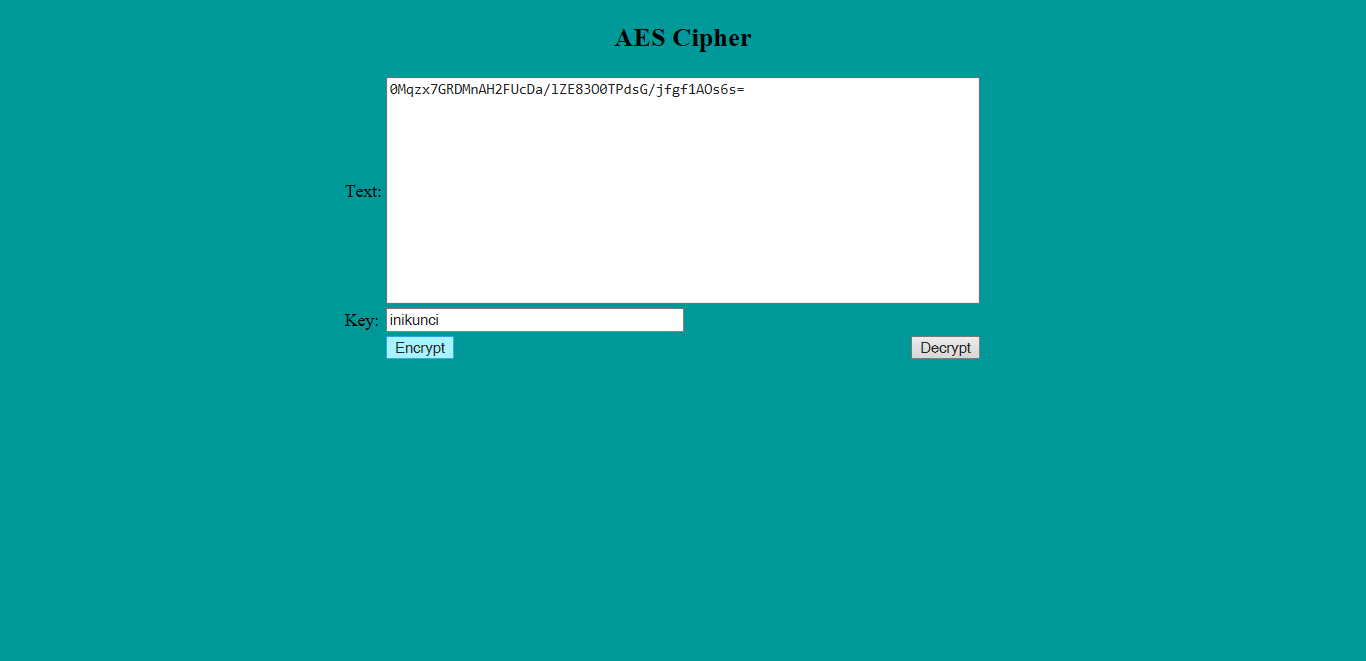
1. Open the php file (localhost/encryption/aes.php)



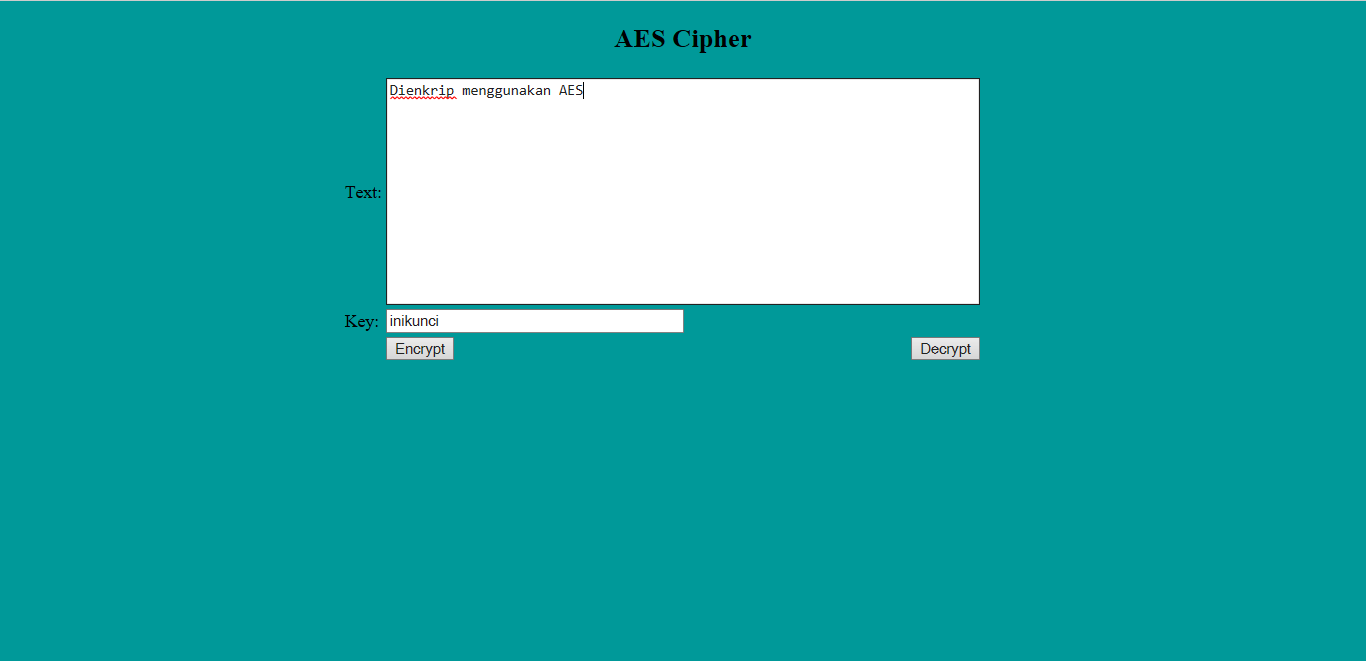
2. Write the plain text that we want to encrypt in the given space labeled “Text”, for example : Dienkrip menggunakan AES. Also input key.



3. After giving both input, click Encrypt button to encrypt the plain text. And will resulting in the following picture.



4. To decrypt it back, give input to the space labeled “Text” with the encrypted text. And the decryption key must be the same as the one being used when encrypting the message. After that, click Decrypt.



5. It would back to the plain text it should be.