

Virtual Lab Practical

DES to 3-DES

Aim: In this experiment, you are asked to design the triple DES cryptosystem provided that you are given an implementation of DES

Manual:

Step 1 : Generate Plaintext m, keyA and keyB by clicking on respective buttons PART I of the simulation page.

PART I

Message:

Key Part A:

Key Part B:

Step 2 : Enter generated Plaintext m from PART I to PART II in "Your text to be encrypted/decrypted:" block.

PART II

Your text to be encrypted/decrypted:

Key to be used:

Output:

Step 3 : Enter generated keyA from PART I to PART II "Key to be used:" block and click on DES encript button to output ciphertext c1.This is First Encryption.

PART II

Your text to be encrypted/decrypted:

Key to be used:

Output:

Step 4 : Enter generated ciphertext c1 from PART II "Output:" Block to PART II in "Your text to be encrypted/decrypted:" block.

PART II

Your text to be encrypted/decrypted:

Key to be used:

Output:

Step 5 : Enter generated keyB from PART I to PART II in "Key to be used:" block and click on

DES decrypt button to output ciphertext c2. This is Second Encryption.

PART II

Your text to be encrypted/decrypted: 00111110 11010100 11010111 01101101 10000110 11100111 00010001 01111111

Key to be used: 922fb510c71f436e

DES Encrypt DES Decrypt

Output: 10101011 10101110 01111110 01111111 01111000 10000100 10011100 10010101

Step 6 : Enter generated ciphertext c2 from PART II "Output:" block to PART II in "Your text to be encrypted/decrypted:" block.

PART II

Your text to be encrypted/decrypted: 10101011 10101110 01111110 01111111 01111000 10000100 10011100 10010101

Key to be used: 922fb510c71f436e

DES Encrypt DES Decrypt

Output: 10101011 10101110 01111110 01111111 01111000 10000100 10011100 10010101

Step 7 : Enter generated keyA from PART I to PART II "Key to be used:" block and click on DES encrypt button to output ciphertext c3. This is Third Encryption. As Encryption is done thrice. This Scheme is called triple DES.

PART II

Your text to be encrypted/decrypted: 10101011 10101110 01111110 01111111 01111000 10000100 10011100 10010101

Key to be used: 3b3898371520f75e

DES Encrypt DES Decrypt

Output: 00011101 11100100 10001000 01101111 11010001 00011011 00110000 11000100

Step 8 : Enter generated ciphertext c3 from PART II "Output:" Block to PART III "Enter your answer here:" block in order to verify your Triple DES.

PART III

Enter your answer here:

00011101 11100100 10001000 01101111 11010001 00011011 00110000 11000100

Check Answer!

CORRECT!

Reference-

<http://cse29-iiith.vlabs.ac.in/exp6/Introduction.html?domain=Computer%20Science&lab=Cryptography%20Lab>

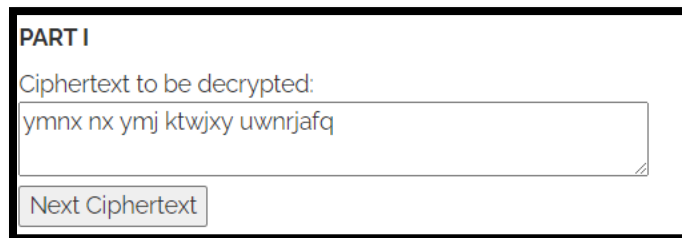
Breaking the shift cipher

Aim: In this experiment, we work with a well-known historical encryption scheme, namely the shift cipher, that has a very small key space.

Your task is to break the shift cipher. Specifically, given (only) the ciphertext in some instance of a shift cipher, you need to find the plaintext and the secret key.

Manual:

STEP 1 : For the given ciphertext in the PART I of the simulation page, the first step is to decrypt it using each of the twenty-six different keys, $k=0,1,\dots,25$ and obtain the corresponding plaintexts. For decryption, you may use the tool given in the PART III of the simulation page.

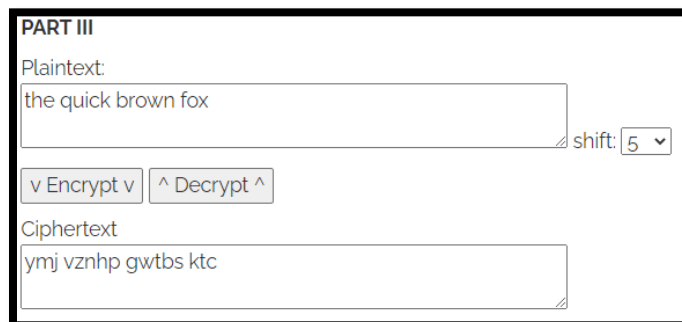


PART I

Ciphertext to be decrypted:

ymnx nx ymj ktwjxy uwnrjafq

Next Ciphertext



PART III

Plaintext:

the quick brown fox

shift: 5

v Encrypt v ^ Decrypt ^

Ciphertext

ymj vznhp gwtbs ktc

STEP 2 : After each decryption, you may cut-and-paste the resultant plaintext in the scratch-pad in the (PART II) of the simulation page, if you need to remember it.

STEP 3 : Finally, observe the plaintexts and choose the most appropriate one (the one that is a meaningful English text) as the recovered plaintext and cut-and-paste it in the text-field named PART IV "Solution Plaintext". Also select the corresponding key in the text-field named "Key" and click on "Check My answer" Button.

PART III

Plaintext:

this is the forest primeval

shift: 5

v Encrypt v ^ Decrypt ^

Ciphertext

ymnx nx ymj ktwjxy uwnrjafq

STEP 4 [OPTIONAL] : Verify that your answer is correct, by encrypting the solution plaintext with your key.

PART IV

Enter your solution Plaintext and shift key here:

this is the forest primeval

Key 5

Check my answer!

CORRECT!!

Reference-

<http://cse29-iiith.vlabs.ac.in/exp1/Introduction.html?domain=Computer%20Science&lab=Cryptography%20Lab>

Digital signature scheme

Aim: In Public key setting, it becomes difficult to verify for a receiver whether message is originated from claimed source.

In this experiment, we show how a receiver can verify integrity of the message in public key setting.

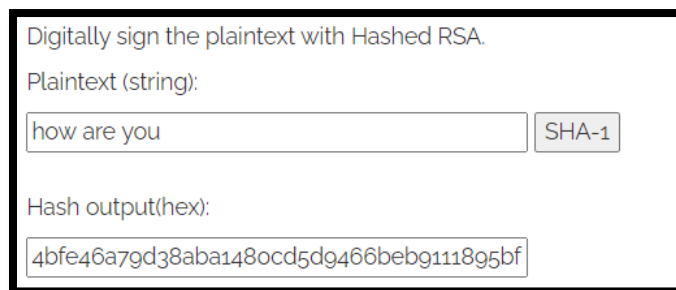
Your task is to verify, whether digital signature scheme really works and why it works?

About:

A Digital Signature is an authentication mechanism that enables the creator of the message to attach a code that acts as a signature. The signature is formed by taking the hash of the message and encrypting the message with the creator's private key. The signature guarantees the source and integrity of the message.

Manual:

Step 1 : Enter the input text to be encrypted in the 'Plaintext' area and generate hash value for message by clicking on the SHA-1 button



Digitally sign the plaintext with Hashed RSA.

Plaintext (string):

how are you

Hash output(hex):

4bfe46a79d38aba1480cd5d9466bebg111895bf

Step 2 : Copy content of Hash Output(hex) field and paste it in Input to RSA(hex) field.



Input to RSA(hex):

4bfe46a79d38aba1480cd5d9466bebg111895bf

Step 3 : Select keysize of public key from RSA Public key section by clicking on any key button.

RSA public key

Public exponent (hex, F4=0x10001):

Modulus (hex):

Here, 512 bit (e=3) is chosen

Step 4 : Click on Apply RSA button to generate a digital signature.

Input to RSA(hex):

Digital Signature(hex):

Digital Signature(base64):

Status:

Reference:

<http://cse29-iiith.vlabs.ac.in/exp10/Introduction.html?domain=Computer%20Science&lab=Cryptography%20Lab>