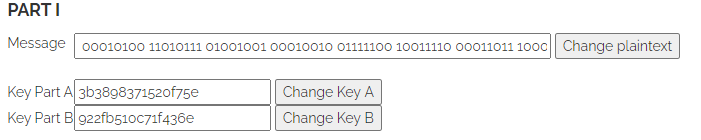
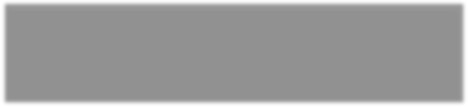
# Virtual Lab Practical

**DES to 3-DES**

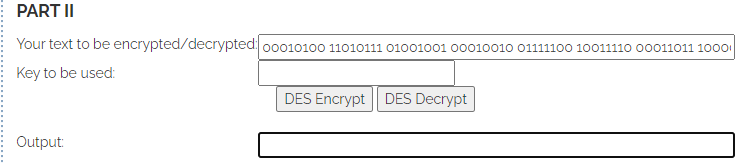
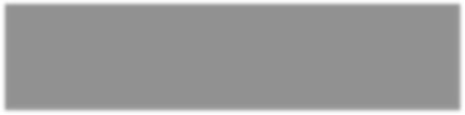
**Aim:** In this experiment, you are asked to design the triple DES cryptosystem provided that you are given an implementation of DES

## Manual:

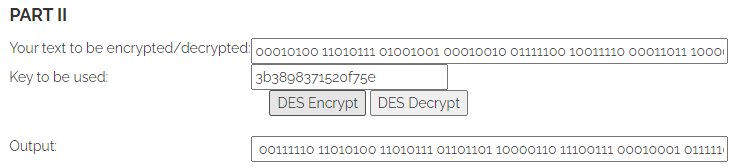
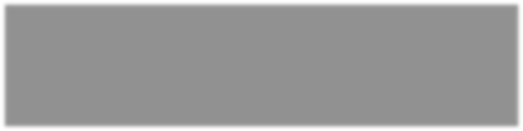
Step 1 : Generate Plaintext m, keyA and keyB by clicking on rexpective buttons PART I of the simulation page.



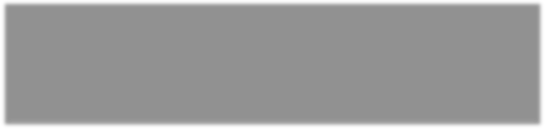
Step 2 : Enter generated Plaintext m from PART I to PART II in "Your text to be encrypted/decrypted:" block.



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

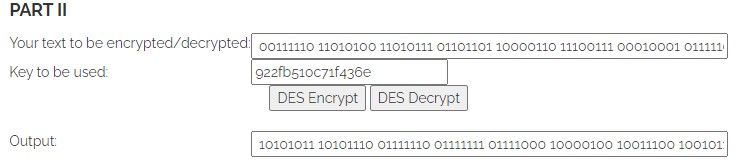
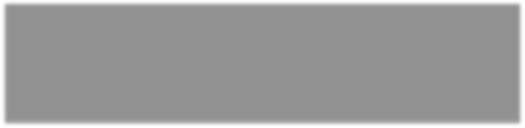


Step 4 : Enter generated ciphertext c1 from PART II "Output:" Block to PART II in "Your text to be encrypted/decrypted:" block.

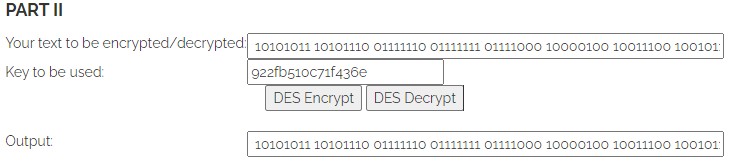
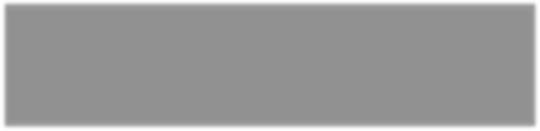


Step 5 : Enter generated keyB from PART I to PART II in "Key to be used:" block and click on

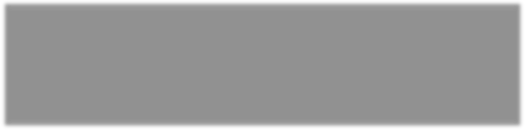
DES decrypt button to output ciphertect c2.This is Second Encryption.



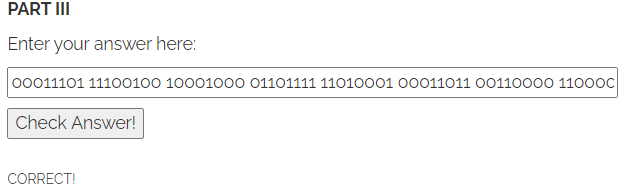
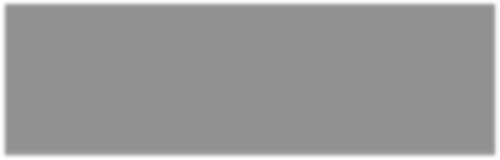
Step 6 : Enter generated ciphertext c2 from PART II "Output:" block to PART II in "Your text to be encrypted/decrypted:" block.



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



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



### Reference-

[http://cse29-](http://cse29-iiith.vlabs.ac.in/exp6/Introduction.html?domain=Computer%20Science&amp;lab=Cryptography%20Lab) [iiith.vlabs.ac.in/exp6/Introduction.html?domain=Computer%20Science&lab=Cryptography%20](http://cse29-iiith.vlabs.ac.in/exp6/Introduction.html?domain=Computer%20Science&amp;lab=Cryptography%20Lab) [Lab](http://cse29-iiith.vlabs.ac.in/exp6/Introduction.html?domain=Computer%20Science&amp;lab=Cryptography%20Lab)

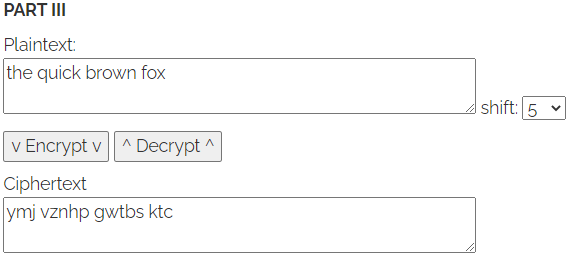
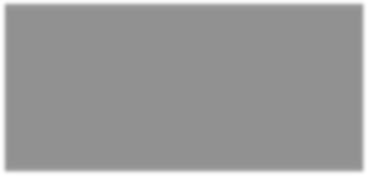
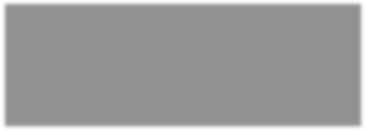
# Breaking the shift cipher

**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:

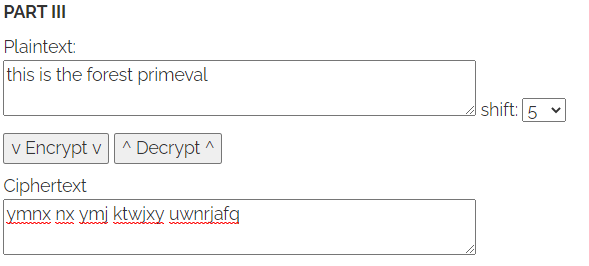
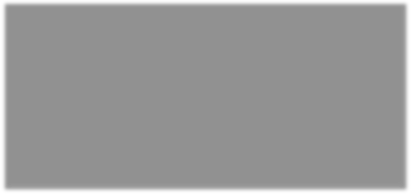
STEP 1 : For the given ciphertext in the PART I of the simulation page, the first step is to decrypt it using each of the twenty-six different keys, k=0,1,...,25 and obtain the corresponding plaintexts. For decryption, you may use the tool given in the PART III of the simulation page.



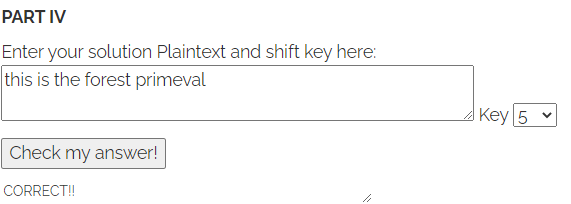
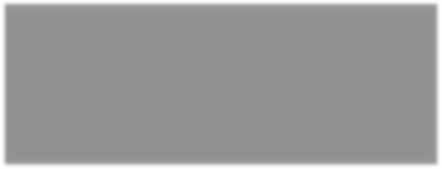
STEP 2 : After each decryption, you may cut-and-paste the resultant plaintext in the scratch-pad in the (PART II) of the simulation page, if you need to remember it.

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.



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



### Reference-

[http://cse29-](http://cse29-iiith.vlabs.ac.in/exp1/Introduction.html?domain=Computer%20Science&amp;lab=Cryptography%20Lab) [iiith.vlabs.ac.in/exp1/Introduction.html?domain=Computer%20Science&lab=Cryptography%20](http://cse29-iiith.vlabs.ac.in/exp1/Introduction.html?domain=Computer%20Science&amp;lab=Cryptography%20Lab) [Lab](http://cse29-iiith.vlabs.ac.in/exp1/Introduction.html?domain=Computer%20Science&amp;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.

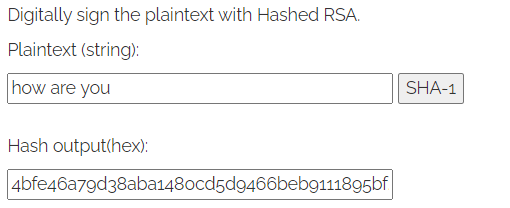
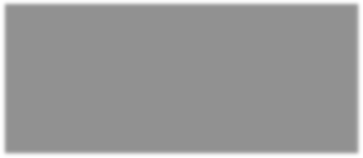
Your task is to verify, whether digital signature scheme really works and why it works?

## About:

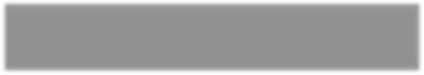
A Digital Signature is an authentication mechanism that enables the creator of the message to attack a code that acts as a signature. The signature is formed by taking the hash of the message and encrypting the message with the creator's private key. The signature guarantees the source and integrity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

## Manual:

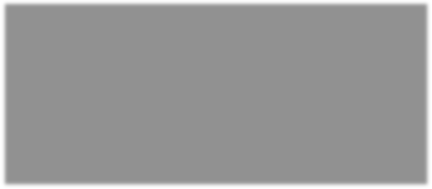
Step 1 : Enter the input text to be encrypted in the 'Plaintext' area and generate hash value for message by clicking on the SHA-1 button



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

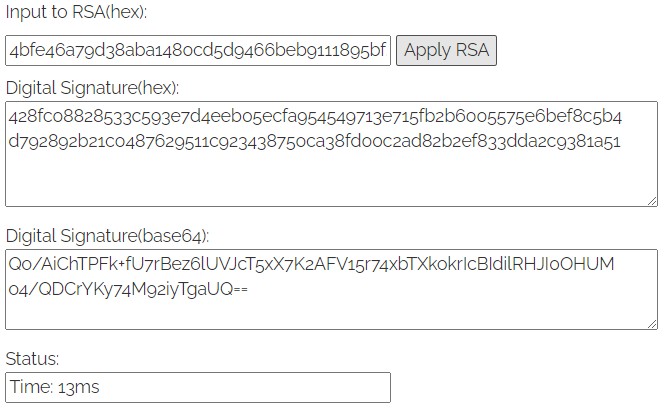
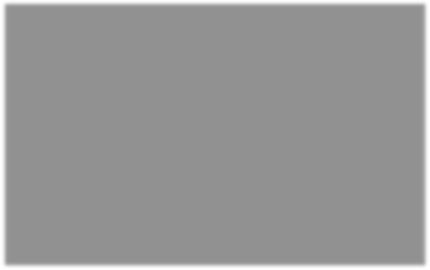


Step 3 : Select keysize of public key from RSA Public key section by clicking on any key button.



Here, 512 bit (e=3) is chosen

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



### Reference:

[http://cse29-](http://cse29-iiith.vlabs.ac.in/exp10/Introduction.html?domain=Computer%20Science&amp;lab=Cryptography%20Lab) [iiith.vlabs.ac.in/exp10/Introduction.html?domain=Computer%20Science&lab=Cryptography%2](http://cse29-iiith.vlabs.ac.in/exp10/Introduction.html?domain=Computer%20Science&amp;lab=Cryptography%20Lab) [0Lab](http://cse29-iiith.vlabs.ac.in/exp10/Introduction.html?domain=Computer%20Science&amp;lab=Cryptography%20Lab)