

# Information Security

## Practical 11: IIT Virtual Cryptography Lab:

URL <https://cse29-iiith.vlabs.ac.in/Experiments.html>

1. Message Authentication Code (CBC-MAC)
2. AES and Modes of Operation
3. Digital Signatures Scheme

### Output:

#### 1) Message Authentication Code (CBC-MAC)

The screenshot shows a web browser window displaying the IIT Virtual Cryptography Lab interface. The URL in the address bar is <https://cse29-iiith.vlabs.ac.in/exp/message-authentication-codes/simulation.html>. The page title is "Message Authentication Code (CBC-MAC)". On the left, there is a sidebar with navigation links: Aim, Theory, Objective, Procedure, Simulation (highlighted), Assignment, References, and Feedback. The main content area contains the following fields and buttons:

- Plaintext:** A text box containing "101010011100111001001" and a "Next Plaintext" button.
- Key, k:** A text box containing "0011100010101111101011000101011000" and a "Next Key" button.
- length of Initialization Vector (IV),  $l$ :** A text box containing "4" and a "Next IV" button.
- IV:** A text box containing "1000" and a "Next IV" button.
- Put your text of size  $l$  to get the corresponding value of  $f_k(\text{text})$  of size  $l$ .**
- Your text:** A text box containing "0001" and an "Apply Function" button.
- Function output:** A text box containing "1000" and a "Choose another Function" button.
- Final Output:** A text box containing "101011010010111100101011" and a "Check Answer!" button.

The Windows taskbar at the bottom shows the search bar, task view button, and several open applications. The system tray on the right shows the battery level at 16%, network status, and the date and time as 11:36 AM on 10/13/2021.

## 2) AES and Modes of Operation [ Cipher Block Chaining]

Virtual Labs

https://cse29-bithvlabz.ac.in/exp/aes/simulation.html

Computer Science and Engineering > Cryptography > Experiments

**Aim**

**Theory**

**Objective**

**Procedure**

**Simulation**

**Assignment**

**References**

**Feedback**

**AES and Modes of Operation**

**AIM I**

Choose your mode of operation: **Cipher Block Chaining**

**AIM II**

Key size: **128**

Plaintext: **ATTACK ON 12/14/2001**

Ciphertext: **00000000000000000000000000000000**

Operation: **Encrypt**

**AIM III**

Calculate KCR:

Plaintext: **00000000000000000000000000000000**

Ciphertext: **00000000000000000000000000000000**

Operation: **Decrypt**

**AIM IV**

Key: **00000000000000000000000000000000**

Plaintext: **00000000000000000000000000000000**

Ciphertext: **00000000000000000000000000000000**

Operation: **Encrypt**

**AIM V**

Enter your chosen key:

**00000000000000000000000000000000**

### 3) AES and Modes of Operation [ Electronic Code Block]

Virtual Labs

https://cse291-lab-vlabs.ac.in/exp/aes/simulation.html

Browse all - Learn... Week 1 - CS50's Int... Wallpaperflare - Be... Important Topic - G... Career Tracks | Data... How to get started... Python Programmi... machine learning... Machine Learning... Other favorite

HOME

AES and Modes of Operation

**PART I**

Choose your mode of operations: **Electronic Code Book (ECB)**

**PART II**

Key size in bits: **128**

Plaintext:  Next Plaintext key:  Next Keytext

**PART IV**

Key in hex:

Plaintext in hex:

Ciphertext in hex:

**PART V**

Enter your answer here:

## 4) AES and Modes of Operation [ Counter Mode]

The screenshot shows the Virtual Labs interface for the experiment 'AES and Modes of Operation'. The browser address bar displays 'https://cse29-iiith.vlabs.ac.in/exp/aes/simulation.html'. The left sidebar contains navigation links: Aim, Theory, Objective, Procedure, Simulation (highlighted), Assignment, References, and Feedback. The main content area is titled 'AES and Modes of Operation' and is divided into five parts:

- PART I:** Choose your mode of operation: Counter Mode (selected).
- PART II:** Key size in bits: 128 (selected).
- PART III:** Plaintext: 4836a08 765a081 6a085a7 61891920  
070a0a 2022234 0a9308 903092  
624875c 3a0c79f 0a0706 67730a9  
077810a 1aa740c 0a0f1a6 0a774a3  
0a330a4 2a9a0a6 61a0a17 0779a01  
Next Plaintext: Key: 3a0c79f 0a0706 67730a9 0a330a4  
Next Keyset
- PART IV:** Calculate XOR:  
XOR: 1780f25 4a2a0a6 3a0c79f 0a0706  
7a0b0a1 3a0c79f 0a0706 67730a9  
XOR: 030a0a4 7a2a0a6 3a0c79f 0a0706
- PART V:** Enter your answer here: 00e10b77 45a0794e 4ae5082 03309c5c 03340414 7a2a34ae 10b0c392 5a03 Check Answer

## 5) AES and Modes of Operation [ Output FeedBack]

The screenshot shows the Virtual Labs interface for the experiment 'AES and Modes of Operation'. The browser address bar displays 'https://cse29-iiith.vlabs.ac.in/exp/aes/simulation.html'. The left sidebar contains navigation links: Aim, Theory, Objective, Procedure, Simulation (highlighted), Assignment, References, and Feedback. The main content area is titled 'AES and Modes of Operation' and is divided into five parts:

- PART I:** Choose your mode of operation: Output Feedback (selected).
- PART II:** Key size in bits: 128 (selected).
- PART III:** Plaintext: 4836a08 765a081 6a085a7 61891920  
070a0a 2022234 0a9308 903092  
624875c 3a0c79f 0a0706 67730a9  
077810a 1aa740c 0a0f1a6 0a774a3  
0a330a4 2a9a0a6 61a0a17 0779a01  
Next Plaintext: Key: 3a0c79f 0a0706 67730a9 0a330a4  
Next Keyset
- PART IV:** Calculate XOR:  
XOR: 1780f25 4a2a0a6 3a0c79f 0a0706  
7a0b0a1 3a0c79f 0a0706 67730a9  
XOR: 030a0a4 7a2a0a6 3a0c79f 0a0706
- PART V:** Enter your answer here: 00e10b77 45a0794e 4ae5082 03309c5c 03340414 7a2a34ae 10b0c392 5a03 Check Answer

## 6) Digital Signature Scheme

The screenshot shows a web browser window with the URL <https://cse29-iitth.vlabs.ac.in/exp/digital-signatures/simulation.html>. The page title is "Digital Signatures Scheme". On the left, there is a navigation menu with links: Theory, Objective, Procedure, Simulation (highlighted), Assignment, References, and Feedback. The main content area displays the following information:

Digitally sign the plaintext with Hashed RSA.

Plaintext (string):

Hash output(hex):

Input to RSA(hex):

Digital Signature(hex):

Digital Signature(base64):

Status:

**RSA public key**

Public exponent (hex,  $P = Q = 10001$ ):

Modulus (hex):

1024 bit | 1024 bit (n=3) | 512 bit | 512 bit (n=3)