19CS3041S – CRYPT ANALYSIS AND CYBER DEFENCE

LAB WORKBOOK

TEAM CACD

KLEF | CRYPT ANALYSIS AND CYBER DEFENCE – 19CS3041S



**LABORATORY WORKBOOK**

|  |  |
| --- | --- |
| STUDENT NAME |  |
| REG. NO |  |
| YEAR |  |
| SEMESTER |  |
| SECTION |  |
| FACULTY |  |

Table of Contents

|  |
| --- |
| 1. **Implementation of Caesar Cipher and Vigenere Cipher** |
| 1. **Implementation of Play Fair encryption and decryption** |
| 1. **Implementation of Hill Cipher encryption and decryption** |
| 1. **Implementation of Rail Fence and Columnar ciphers** |
| 1. **Implementation of S-DES algorithm** |
| 1. **Implementation of Substitute bytes, Shift rows operations in AES** |
| 1. **Implementation of LCG, and Blum-Blum Sub generators** |
| 1. **Implementation of simplified RC4** |
| 1. **Implementation of RSA Algorithm** |
| 1. **Implementation of Diffie-Hellman Algorithm** |
| 1. **Implementation of Elgamal Crypto System Algorithm** |
| 1. **Implementation of Simple hash algorithm** |

**Organization of the STUDENT LAB WORKBOOK**

The laboratory framework includes a creative element but shifts the time-intensive aspects outside of the Two-Hour closed laboratory period. Within this structure, each laboratory includes three parts: Prelab, In-lab, and Post-lab.

* 1. **Pre-Lab**

The Prelab exercise is a homework assignment that links the lecture with the laboratory period - typically takes 2 hours to complete. The goal is to synthesize the information they learn in lecture with material from their textbook to produce a working piece of software. Prelab Students attending a two-hour closed laboratory are expected to make a good-faith effort to complete the Prelab exercise before coming to the lab. Their work need not be perfect, but their effort must be real (roughly 80 percent correct).

* 1. **In-Lab**

The In-lab section takes place during the actual laboratory period. The First hour of the laboratory period can be used to resolve any problems the students might have experienced in completing the Prelab exercises. The intent is to give constructive feedback so that students leave the lab with working Prelab software - a significant accomplishment on their part. During the second hour, students complete the In-lab exercise to reinforce the concepts learned in the Prelab. Students leave the lab having received feedback on their Prelab and In-lab work.

* 1. **Post-Lab**

The last phase of each laboratory is a homework assignment that is done following the laboratory period. In the Post-lab, students analyse the efficiency or utility of a given system call. Each Post-lab exercise should take roughly 120 minutes to complete.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **S. No** | **Date** | **Experiment Name** | **Pre-Lab (5M)** | **In-Lab** | | | | **Post Lab (5M)** | **Viva**  **Voce**  **(5M)** | **Total (50M)** | **Faculty Signature** |
| **LOGIC (10M)** | **EXECUTION (10M)** | **RESULT (10M)** | **ANALYSIS (5M)** |
| 1 |  |  |  |  |  |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |  |  |  |  |  |
| 4 |  |  |  |  |  |  |  |  |  |  |  |
| 5 |  |  |  |  |  |  |  |  |  |  |  |
| 6 |  |  |  |  |  |  |  |  |  |  |  |
| 7 |  |  |  |  |  |  |  |  |  |  |  |
| 8 |  |  |  |  |  |  |  |  |  |  |  |
| 9 |  |  |  |  |  |  |  |  |  |  |  |
| 10 |  |  |  |  |  |  |  |  |  |  |  |
| 11 |  |  |  |  |  |  |  |  |  |  |  |
| 12 |  |  |  |  |  |  |  |  |  |  |  |

**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

**SUBJECT CODE: 19CS3041S**

**CRYPT ANALYSIS AND CYBER DEFENCE WORKBOOK**

# 1. Implementation of Caesar Cipher and Vigenère Cipher.

**Date of the Session: \_\_\_/\_\_\_/\_\_\_ Time of the Session: \_\_\_\_\_to\_\_\_\_\_\_**

## **Learning Outcomes:**

* To understand the concept of Encryption and Decryption.
* To understand the applications of substitution techniques.
* To understand Symmetric Crypto System.

**Pre-Lab Task:**

1. Define Cryptography and write any two applications of cryptography.
2. What are the different types of Cryptographic Algorithms?
3. Mention the cryptographic algorithm used in Blockchain Technology and

Gmail.

1. What is the need for encryption?
2. Define symmetric cryptography and Asymmetric cryptography.

**In-Lab Task:**

1. Write a program to implement Caesar Cipher(encryption/decryption) for any given plain text.

*(Hint: As a sample input student need to use his/her name as an input for implementing the program. Shift pattern to be taken as 4)*

2.Write a program to implement Vigenère Cipher(encryption/decryption) for any given plain text.

*(Hint: As a sample input student need to use his/her name as an input for implementing the program. Key to be considered as your choice not exceeding the size 4 )*

Sol:

**Post Lab Task:**

1. Write a pseudo code for encryption and decryption using Caesar Cipher and Vigenère Cipher technique.

*(For Evaluator’s use only)*

|  |  |
| --- | --- |
| Comment of the Evaluator (if Any) | Evaluator’s Observation  Marks Secured: \_\_\_\_\_\_\_\_out of \_\_\_\_\_\_\_\_\_  Full Name of the Evaluator:  Signature of the Evaluator Date of Evaluation |

**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

**SUBJECT CODE: 19CS3041S**

**CRYPT ANALYSIS AND CYBER DEFENCE WORKBOOK**

# 2. Implementation of Playfair Cipher substitution technique

**Date of the Session: \_\_\_/\_\_\_/\_\_\_ Time of the Session: \_\_\_\_\_to\_\_\_\_\_\_**

## **Learning Outcomes:**

* To understand the concept of multiple-letter encryption.
* To understand the applications of the technique.

**Pre-Lab Task:**

1.Define digram with an example.

2.What is the reason to consider a 5 × 5 matrix in a playfair cipher technique?

3.What to do if letters in plain text reoccur eg: *Hello*?

4.What are the advantages of Playfair cipher?

5. Trace what will be the encrypted message by using Playfair cipher if the message is ‘balloon’ and the key is “Monarchy”.

**In-Lab Task:**

1) Write a code to implement Playfair Cipher Substitution Technique for the following input:

Sample Input:-

Plain Text: “Student to consider his/her name”

Secret Key: REDHATCLUB

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| R | E | D | H | A |
| T | C | L | U | B |
| F | G | I/J | K | M |
| N | O | P | Q | S |
| V | W | X | Y | Z |

*(****Note****: Ignore the whitespace and consider the text)*

**Post-Lab Task:**

1) Write a Pseudocode for Playfair Cipher Substitution technique.

Sol)

*(For Evaluator’s use only)*

|  |  |
| --- | --- |
| Comment of the Evaluator (if Any) | Evaluator’s Observation  Marks Secured: \_\_\_\_\_\_\_\_out of \_\_\_\_\_\_\_\_\_  Full Name of the Evaluator:  Signature of the Evaluator Date of Evaluation |

**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

**SUBJECT CODE: 19CS3041S**

**CRYPT ANALYSIS AND CYBER DEFENSE WORKBOOK**

# 3. Implementation of Hill Cipher Substitution technique

**Date of the Session: \_\_\_/\_\_\_/\_\_\_ Time of the Session: \_\_\_\_\_to\_\_\_\_\_\_**

## **Learning Outcomes:**

* To understand the concept multilettered encryption and decryption.
* To understand the applications of substitution techniques.

**Pre-Lab Task:**

1. Hill Cipher is a block cipher. Justify.
2. If A= , find |A|.

3. Write the mathematical formula for encryption and decryption in Hill Cipher.

4. If A = , find A-1.

5. Can we consider the matrix as a key matrix in Hill Cipher. Justify.

**In-Lab Task:**

Q.1) Write a program to implement Hill Cipher Substitution technique for the following input.

**Sample Input:**

***Plain Text:*** *Student to consider His/Her name*

***Key:*** *ALBO*

*Note: White space in the plaintext can be ignored and the key matrix must be 2×2 matrix.*

*Filer character to be taken as ‘x’.*

Sol)

**Post-Lab Task:**

1. Write a Pseudocode to find the inverse of a 3×3 matrix.

*(For Evaluator’s use only)*

|  |  |
| --- | --- |
| Comment of the Evaluator (if Any) | Evaluator’s Observation  Marks Secured: \_\_\_\_\_\_\_\_out of \_\_\_\_\_\_\_\_\_  Full Name of the Evaluator:  Signature of the Evaluator Date of Evaluation |

**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

**SUBJECT CODE: 19CS3041S**

**CRYPT ANALYSIS AND CYBER DEFENCE WORKBOOK**

# 4. Transposition and Columnar Techniques

**Date of the Session: \_\_\_/\_\_\_/\_\_\_ Time of the Session: \_\_\_\_\_to\_\_\_\_\_\_**

## **Learning Outcomes:**

* To understand the concept of Encryption and Decryption.
* To understand the applications of Transposition techniques
* To understand the applications of Columnar techniques

**Pre-Lab Task:**

1. What is transposition cipher?
2. What are the applications of rail-fence cipher?
3. Brief description of columnar transposition cipher.
4. Columnar transposition cipher is also known as\_\_\_\_\_\_\_\_\_\_\_.
5. How to break a rail-fence cipher?

**In-Lab Task:**

1. Write a program to implement Rail-Fence Cipher (encryption/decryption) for any given plain text.

Sample input: - N=6 Message=S21location56

Sample output: - Si2to1anac5to6l

**Post Lab Task:**

1. Write a pseudo code for encryption and decryption using Rail Fence Cipher.

*(For Evaluator’s use only)*

|  |  |
| --- | --- |
| Comment of the Evaluator (if Any) | Evaluator’s Observation  Marks Secured: \_\_\_\_\_\_\_\_out of \_\_\_\_\_\_\_\_\_  Full Name of the Evaluator:  Signature of the Evaluator Date of Evaluation |

**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

**SUBJECT CODE: 19CS3041S**

**CRYPT ANALYSIS AND CYBER DEFENSE WORKBOOK**

# 5. Simplified - Data Encryption Standard Algorithm

**Date of the Session: \_\_\_/\_\_\_/\_\_\_ Time of the Session: \_\_\_\_\_to\_\_\_\_\_\_**

## **Learning Outcomes:**

* To understand symmetric key block cipher technique.
* To apply S-DES algorithm for key generation, Encryption and Decryption.

**Pre-Lab Task:**

1. Discuss on the size of Plain text, Cipher text and Key for general DES algorithm.

2. Apply S-DES algorithm and generate key followed by encryption and decryption.

**Input:**

**Plain Text (8 - bits):** Use the binary equivalent of the last Number of your register number.

*Test case: If the last number is 0, then consider the predecessor non-zero value.*

***Initial Permutation: 2 6 3 1 4 8 5 7***

***Expanded Permutation: 4 1 2 3 2 3 4 1***

***S = S =***

***P4: 2 4 3 1***

**Key (10 – bits) : 1 1 0 1 0 0 0 0 0 1**

***P10 order:*** *3 5 2 7 4 10 1 9 8 6*

***P8 order:*** *6 3 7 4 8 5 10 9*

**In-Lab Task:**

1.Consider the example that was solved in your Prelab, take those as the inputs and implement the algorithm using Java/Python.

**Post Lab:**

1. Write a Pseudocode to implement key generation using S-DES algorithm.

*(For Evaluator’s use only)*

|  |  |
| --- | --- |
| Comment of the Evaluator (if Any) | Evaluator’s Observation  Marks Secured: \_\_\_\_\_\_\_\_out of \_\_\_\_\_\_\_\_\_  Full Name of the Evaluator:  Signature of the Evaluator Date of Evaluation |

**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

**SUBJECT CODE: 19CS3041S**

**CRYPT ANALYSIS AND CYBER DEFENCE WORKBOOK**

# 6. Implementation of Substitute bytes and Shift rows operations in AES.

**Date of the Session: \_\_\_/\_\_\_/\_\_\_ Time of the Session: \_\_\_\_\_to\_\_\_\_\_\_**

## **Learning Outcomes:**

* To use S-Box to perform a byte-by-byte substitution of the block.
* To understand shift row operation using permutation.

**Pre-Lab Task:**

1. How many keys are used in AES with respective to key size? And how many rounds are there in AES?
2. Why AES is better than DES, Double DES, Triple DES?
3. How many rounds will take place if it 128bit, 192bit, and 256bit respectively?
4. Name the methods present in AES transformation function.

**In-Lab Task:**

1. Siri is a part of cryptanalysis team in an organization. The team is developing a complete application to decrypt a message using AES algorithm, the team lead has given ‘Shift Rows Module’ to Siri. To complete this module Siri asked you to write a program which performs shift rows operation in AES algorithm. Write the code by following the Input and Output Format given below:

|  |  |  |  |
| --- | --- | --- | --- |
| Si(0,0) | Si(0,1) | Si(0,2) | Si(0,3) |
| Si(1,0) | **Si(1,1)** | **Si(1,2)** | **Si(1,3)** |
| Si(2,0) | **Si(2,1)** | **Si(2,2)** | **Si(2,3)** |
| Si(3,0) | **Si(3,1)** | **Si(3,2)** | **Si(3,3)** |

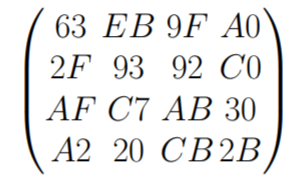
**Input Format:** 4X4 matrix will be given as input

|  |  |  |  |
| --- | --- | --- | --- |
| So(0,0) | So(0,1) | So(0,2) | So(0,3) |
| So(1,1) | **So1,2)** | **So(1,3)** | **So(1,0)** |
| So(2,2) | **So(2,3)** | **So(2,0)** | **So(2,1)** |
| So(3,3) | **So(3,0)** | **So(3,1)** | **So(3,2)** |

**Output Format:** 4x4 matrix after performing shift-row operations

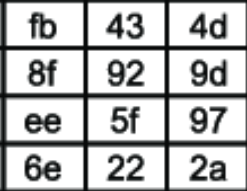
**Post Lab Task:**

1) Given below is a state matrix, now you have to perform inverse shift rows for the given state matrix to help your friend decrypt.



Help your friend to write a Pseudocode to perform Inverse Shift Rows transformation.

Use the above table to perform Substitute Bytes Transformation operation in AES.



*(For Evaluator’s use only)*

|  |  |
| --- | --- |
| Comment of the Evaluator (if Any) | Evaluator’s Observation  Marks Secured: \_\_\_\_\_\_\_\_out of \_\_\_\_\_\_\_\_\_  Full Name of the Evaluator:  Signature of the Evaluator Date of Evaluation |

**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

**SUBJECT CODE: 19CS3041S**

**CRYPT ANALYSIS AND CYBER DEFENCE WORKBOOK**

# 7. Implementation LCG and Blum-Blum Sub generators

# Date of the Session: \_\_\_/\_\_\_/\_\_\_ Time of the Session: \_\_\_\_\_to\_\_\_\_\_\_

## **Learning Outcomes:**

* To understand and implement Pseudo random number generation.
* To generate secure pseudorandom generators using Blum Blum Shub generator.

**Pre-Lab Task:**

1. Why linear congruential pseudo random number generator shall not be used in cryptosystems?

2. How can we find the period of LCG?

3. Explain Blum Blum Shub sub generator in terms of security.

4. In Blum Blum Shub Generator, do we require to hide the prime factors p,q of the Modulus N?

**In-Lab Task:**

1. Rajesh is working in security domain of a company, his task is to secure the data using different cryptographic algorithm. Help Rajesh in generating an RC4 key using Blum Blum Shub generator.

**Post Lab Task:**

1. Ritish is working on Linear Congruential Generators to generate a series of random numbers for seed X0 = 1073 and parameters a = 35, c = 528 and m = 2547 as given. Write the series of random numbers using linear congruential generators.

*(For Evaluator’s use only)*

|  |  |
| --- | --- |
| Comment of the Evaluator (if Any) | Evaluator’s Observation  Marks Secured: \_\_\_\_\_\_\_\_out of \_\_\_\_\_\_\_\_\_  Full Name of the Evaluator:  Signature of the Evaluator Date of Evaluation |

**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

**SUBJECT CODE: 19CS3041S**

**CRYPT ANALYSIS AND CYBER DEFENCE WORKBOOK**

# 8. Implementation of simplified RC4.

# Date of the Session: \_\_\_/\_\_\_/\_\_\_ Time of the Session: \_\_\_\_\_to\_\_\_\_\_\_

## **Learning Outcomes:**

* To understand variable key size stream cipher with byte oriented operations.
* To understand random permutation concept.

**Pre-Lab Task:**

1. What are the pros and cons of RC4?
2. Is RC4 better than AES? Justify your answer.

3. Write short notes on stream generation.

**In-Lab Task:**

1. After the second apocalypse on earth no one survived except 5 who went to space in a spaceship: Clarke , Bellamy , Revan , Murphy and Echo . After 20 years of the apocalypse they surprisingly got an encrypted text message from earth, no one understood the message. Clarke expected that the message is encrypted by RC4 method and asked Revan to decrypt the message. So , write a python program to decrypt the RC4 encrypted text by giving key and text as user input.

Message from earth : “  **AEB19F4906E2717ADA765DDC5D21F336C84F98** ”

Key:   **Can be considered as your choice.**

**Post Lab Task:**

1. Write a Pseudo code for the encryption and decryption of RC4.

*(For Evaluator’s use only)*

|  |  |
| --- | --- |
| Comment of the Evaluator (if Any) | Evaluator’s Observation  Marks Secured: \_\_\_\_\_\_\_\_out of \_\_\_\_\_\_\_\_\_  Full Name of the Evaluator:  Signature of the Evaluator Date of Evaluation |

**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

**SUBJECT CODE: 19CS3041S**

**CRYPT ANALYSIS AND CYBER DEFENCE WORKBOOK**

# 9. Implementation of RSA Algorithm

# Date of the Session: \_\_\_/\_\_\_/\_\_\_ Time of the Session: \_\_\_\_\_to\_\_\_\_\_\_

## **Learning Outcomes:**

* To implement RSA algorithm.
* To understand encryption as a block.

**Pre-Lab Task:**

1.What is Asymmetric key? Explain Public and Private keys in RSA.

2.What is Eulers totient? Generate Eulers totient for the given numbers:

i) P=101, Q=173

3.Encrypt the following message using RSA Algorithm.

Message = CSE

**In-Lab Task:**

1. Write a program to implement RSA Algorithm for the following input.

Sample Input:

*Note: you can use CACD as “03010304”*

**Post Lab Task:**

1. University decided to make their communications more secure by better encryption technique. So according to trend RSA algorithm is one of the strongest encryption techniques and they finalized it. They want this work done by students, so to find students who are interested in it they gave a challenge to their students to encrypt a message "Hi" with RSA algorithm and submit it so they can find the best now. Its time for you to submit the implementation of encryption using RSA algorithm.

*(For Evaluator’s use only)*

|  |  |
| --- | --- |
| Comment of the Evaluator (if Any) | Evaluator’s Observation  Marks Secured: \_\_\_\_\_\_\_\_out of \_\_\_\_\_\_\_\_\_  Full Name of the Evaluator:  Signature of the Evaluator Date of Evaluation |

**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

**SUBJECT CODE: 19CS3041S**

**CRYPT ANALYSIS AND CYBER DEFENCE WORKBOOK**

# 10. Implementation of Diffie-Hellman Algorithm

# Date of the Session: \_\_\_/\_\_\_/\_\_\_ Time of the Session: \_\_\_\_\_to\_\_\_\_\_\_

## **Learning Outcomes:**

* To understand the key exchange process.
* To understand the purpose of Discrete Logarithms.

**Pre-Lab Task:**

1. What is the difference between RSA and Diffie Hellman?

2.What are the main properties of Diffie Hellman?

3.Explain Asymmetric key cryptography in few words and draw a neat diagram on its working.

**In-Lab Task:**

1. You are trying to encrypt your messages you want to send to your friend because you don’t want an outsider to know the confidential information you are sending to your friend so in order to do that use Diffie-Hellman Algorithm to encrypt the messages(choose an appropriate example) and encrypt the messages using Diffie-Hellman Algorithm.

**Post Lab Task:**

1. Suppose that two parties A and B wish to set up a common secret key (D-H key) between themselves using the Diffie Hellman key exchange technique. They agree on 7 as the modulus and 3 as the primitive root. Party A chooses 2 and party B chooses 5 as their respective secrets. Find the Diffie Hellman key.

*(For Evaluator’s use only)*

|  |  |
| --- | --- |
| Comment of the Evaluator (if Any) | Evaluator’s Observation  Marks Secured: \_\_\_\_\_\_\_\_out of \_\_\_\_\_\_\_\_\_  Full Name of the Evaluator:  Signature of the Evaluator Date of Evaluation |

**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

**SUBJECT CODE: 19CS3041S**

**CRYPT ANALYSIS AND CYBER DEFENCE WORKBOOK**

# 11. Implementation of Elgamal Cryptosystem Algorithm

# Date of the Session: \_\_\_/\_\_\_/\_\_\_ Time of the Session: \_\_\_\_\_to\_\_\_\_\_\_

## **Learning Outcomes:**

* To understand asymmetric key encryption algorithm for public key cryptography.
* To set up a secure channel between the sender and receiver.

**Pre-Lab Task:**

1. List out the disadvantages of Public key Cryptography/

2.Define Multiplicative group with an example.

3.Summarize the applications of Elgamal Cryptosystem.

**In-Lab Task:**

1. Implement **Elgamal cryptosystem in Python for the original message “I am using Elgamal encryption” and print the decrypted message.**

**Post Lab Task:**

1. Write a Pseudocode for Elgamal cryptosystem.

*(For Evaluator’s use only)*

|  |  |
| --- | --- |
| Comment of the Evaluator (if Any) | Evaluator’s Observation  Marks Secured: \_\_\_\_\_\_\_\_out of \_\_\_\_\_\_\_\_\_  Full Name of the Evaluator:  Signature of the Evaluator Date of Evaluation |

**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

**SUBJECT CODE: 19CS3041S**

**CRYPT ANALYSIS AND CYBER DEFENCE WORKBOOK**

# 12. Implementation a Simple hash algorithm

# Date of the Session: \_\_\_/\_\_\_/\_\_\_ Time of the Session: \_\_\_\_\_to\_\_\_\_\_\_

## **Learning Outcomes:**

* To understand the importance of Hash function for secure data transmission.
* To analyse the difference between SHA and other traditional security algorithms.

**Pre-Lab Task:**

1) What is SHA Algorithm?

2) What is the hash value of SHA-1?

3) Write any 3 differences between SHA-1 and SHA-256?

Q4) What is SHA256 hash function?

**In-Lab Task:**

1. Kiran is doing an internship in Cyber Security. As part of his research, he is assigned a task to demonstrate the working of SHA algorithm in Computer programming language.

**Post Lab Task:**

1. As Raj groups is using SHA1, SHA256 Hash functions. Help Raj friend Ravi to implement different Hash Functions (SHA-512, MD5)

*(For Evaluator’s use only)*

|  |  |
| --- | --- |
| Comment of the Evaluator (if Any) | Evaluator’s Observation  Marks Secured: \_\_\_\_\_\_\_\_out of \_\_\_\_\_\_\_\_\_  Full Name of the Evaluator:  Signature of the Evaluator Date of Evaluation |