

**EVALUATION OF INTERNSHIP REPORT**

## B.Tech: III Year

**Department of Computer Science & Information Technology**

**Name of the Student: Honey Sharma**

**Branch & section: CSIT-2**

**Roll No: 0827CI201078**

**Year: 2022-2023**

## Department of Computer Science & Information Technology

**AITR, Indore**

**ACROPOLIS INSTITUTEOF TECHNOLOGY &RESEARCH, INDORE**

# Department of Computer Science & Information Technology

**Certificate**

Certified that training work entitled “Cyber Security” is a beneficed work carried out after sixth semester by *Honey Sharma* in partial fulfillment for the award of the degree of Bachelor of Technology in Computer Science and Information Technology from *Prof. Nidhi Nigam* Acropolis Institute of Technology and Research during the academic year 2022-23.

*Prof. Nidhi Nigam*

**ACROPOLIS INSTITUTE OF TECHNOLOGY & RESEARCH, INDORE**

# Department of Computer Science & Information Technology

**ACKNOWLEDGEMENT**

I would like to acknowledge the contributions of the following people without whose help and guidance this report would not have been completed. I acknowledge the counsel and support of our training **Prof. Nidhi Nigam**, CSIT Department, with respect and gratitude, whose expertise, guidance, support, encouragement, and enthusiasm has made this report possible. Their feedback vastly improved the quality of this report and provided an enthralling experience. I am indeed proud and fortunate to be supported by him/her. I am also thankful to Dr. Shilpa Bhalerao, H.O.D of Computer Science Information Technology Department, for her constant encouragement, valuable suggestions and moral support and blessings. Although it is not possible to name individually, I shall ever remain indebted to the faculty members of CSIT Department, for their persistent support and cooperation extended during this work.

*Honey Sharma*

*0827CI201078*

### ACROPOLIS INSTITUTE OF TECHNOLOGY & RESEARCH, INDORE

### INDEX

S.no CONTENTS Page no.

1. Introduction to technology Undertaken 1

2. Objectives 2

3. Project undertaken 3

4. Screenshots of Project and Certificates . 6

5. Github Links 8

7. Conclusion 8

8. References/ Bibliography 8

* **Introduction to technology Undertaken :**

JAVA, AES, Cyber Security

Java has introduced a new approach in the technology sector as a programming language. Java takes the top spot of technologies used for coding. A Java application design firm can do everything from comprehensive business software to apps for mobile phones and wireless devices.

Omnipresent of this Software support is always there to get embedded through functioning methods and has been incorporated into common internet browsers. It implies that a similar key is utilized for both encryption and decoding. The (AES) is a generally utilized key encryption calculation.

Securing data transfer is done in multiple ways. But most experts refer to data encryption as the best method and currently, Java AES is an advanced solution available for ciphering. New algorithms are replacing the old values of DES towards the AES. It has a better legacy of confidential properties, data authentication, and high levels of integrity.

* **Objective:**

Cryptography is the practice and study of techniques for secure communication in the presence of third parties called adversaries. More generally, cryptography is about constructing and analyzing protocols that prevent third parties or the public from reading private messages; various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation are central to modern cryptography. Modern cryptography exists at the intersection of the disciplines of mathematics, computer science, electrical engineering, communication science, and physics. Applications of cryptography include electronic commerce, chip-based payment cards, digital currencies, computer passwords, and military communications.

As cyber security concerns arise, the use of AES as an advanced method strikes as the best alternative as it has 3 blocks cipher. They can scramble the 128-bit block with cryptographic keys. Both the sender and receiver possess the same key in order to keep information classified and secretive. This makes it a flexible and safe tool. It works in a block mode which is fixed or stream mode which uses bits of data. Currently, the applications are common for email communications, TLS, and also instant messaging.

* **Project Undertaken:**

**Encryption Decryption (Cipher Text)**

Data encryption is an important feature in data protection. There are various methods used to encrypt and decrypt data to enhance the safety of data transmitted.

The primary purpose of encryption is to protect the confidentiality of digital data stored on computer systems or transmitted over the internet or any other computer network. In addition to security, the adoption of encryption is often driven by the need to meet compliance regulations.

The purpose of encryption is confidentiality concealing the content of the message by translating it into a code. The purpose of digital signatures is integrity and authenticity verifying the sender of a message and indicating that the content has not been changed.

**An overview of AES algorithm:**

AES is a 128-bit symmetric block cipher text. This algorithm uses substitution and permutations; known as the SP networks. It consists of multiple texts to produce a cipher text. AES performs its calculations in the form of byte data instead of bit data.

This means that AES treats 128 bits of a clear text block as 16 bytes. The number of rounds during the encryption process depends on the key size being used.

For example:

* The 128-bit key size uses 10 rounds.
* The 192-bit key size uses 12 rounds.
* The 256-bit key size uses 14 rounds.

Data to be encrypted is stored in a 4 by 4 matrix format called the state array.

Each output takes a state array as input and gives a similar array as output.

In a 16-bytes matrix, each cell represents 1-byte, this means that four cells which

Is the equivalent of four bytes represent one word, implying that each state array

Has four words.

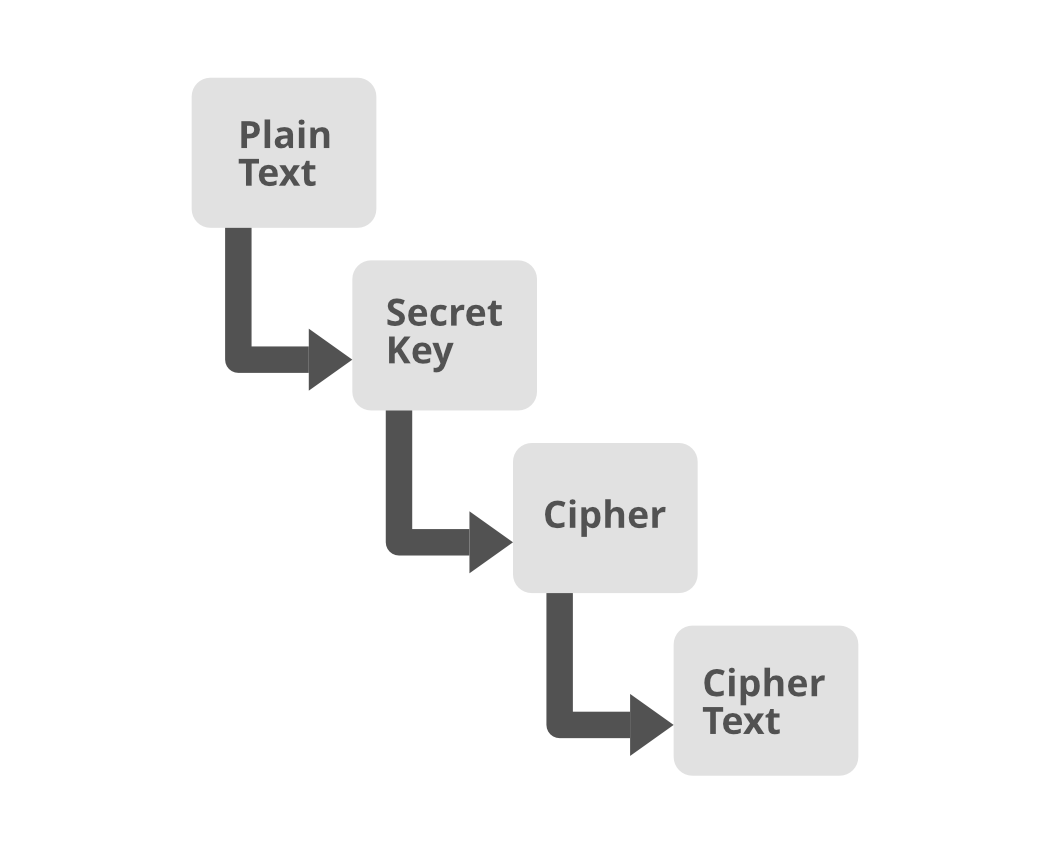
In the block cipher mode, the plain text is converted into block size for

encrypting. Here padding is required and Java provides 3 alternatives. For

encoding, the AES algorithm is repetitive in nature and supports 128, 192, and

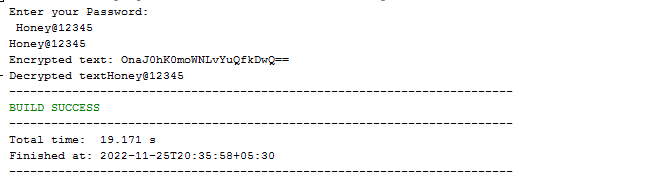
256 bits.

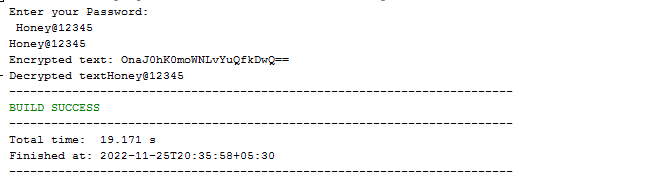
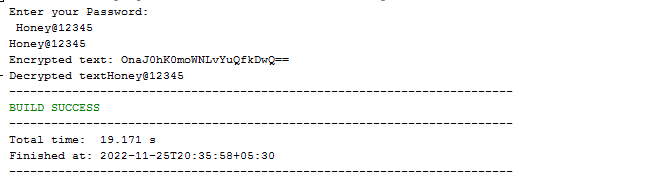
It functions like the below pattern.



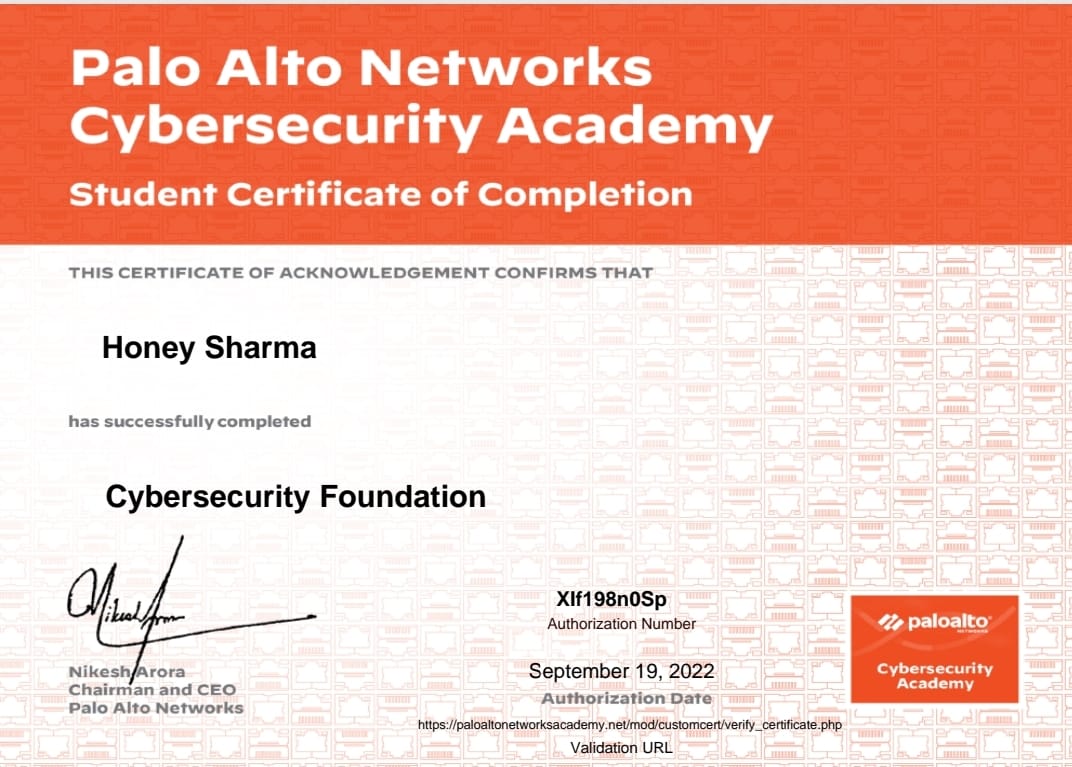
* **Screenshots of Project :**

Output:

****

** **

* **Certificates**



* **GitHub Links :**

<https://github.com/honeyy02/Evaluation_of_Internship-EOI->

* **Conclusion**

Encryption is essential to keep private information, messages, and financial transactions private and secure in a digital world. It protects the confidentiality of digital data stored on computer systems or transmitted over the internet. Various types of encryption techniques are available including the Advanced Encryption Standard (AES), the gold standard for data encryption, used worldwide and the U.S. government standard.

With Java cryptography, it is easy to develop an algorithm that can be used to protect our data from unauthorized access. This is enabled by the Java packages that allow the user to import and develop an algorithm that they can use.

* **References**

[www.google.com](http://www.google.com)

[www.youtube.com](http://www.youtube.com)

<https://en.wikipedia.org/wiki/Computer_security>