NITTE EDUCATION TRUST | N.M.A.M. INSTITUTE OF TECHNOLOGY
(An Autonomous Institution affiliated to Visvesvaraya Technological University, Belagavi)
Nitte – 574 110, Karnataka, India

REPORT

ON

FOUR MONTHS OF INTERNSHIP

Carried out at

AAVISHK SUSTAINABLE SOLUTIONS PVT LTD.

Submitted to

NMAM INSTITUTE OF TECHNOLOGY, NITTE

(An Autonomous Institution under VTU, Belagavi)

In partial fulfillment of the requirements for the award of the

Degree of Bachelor of Engineering

in

Computer Science & Engineering

by

K SHESHADRI PAI

USN: **4NM19CS088**

Under the guidance of

Mr. Sahil Bhanastarkar

NITTE EDUCATION TRUST | N.M.A.M. INSTITUTE OF TECHNOLOGY
(An Autonomous Institution affiliated to Visvesvaraya Technological University, Belagavi)
Nitte – 574 110, Karnataka, India

CERTIFICATE

This is to certify that the "Internship report" submitted by Mr. K SHESHADRI PAI bearing USN 4NM19CS088 *of* 8th *semester B.E., a bonafide student of NMAM Institute of Technology, Nitte, has undergone four months of internship at* AAVISHK SUSTAINABLE SOLUTIONS PVT LTD. *during* April 2022 – August 2022 *fulfilling the partial requirements for the award of degree of Bachelor of Engineering in* ***Computer Science & Engineering*** *at NMAM Institute of Technology, Nitte.*

Name and Signature of Mentor

Ankitha Nayak

Signature of HOD

INDUSTRY CERTIFICATE

Aavishk Sustainable Solutions Pvt Ltd
#10,"Vinyasa", Cambridge Road,
Ulsoor, Bangalore 560 008, India
Mob: +91 9845845386 / Tel: +91 8025540221
tejas.sati@aavishk-tech.com / tejas.sati@gmail.com
CIN U37200KA2015PTC078715

AAvishK

DELIVERING SUSTAINABLE ALTERNATIVES

09-08-2022

CERTIFICATE

This is to inform you that **Mr. Sheshadri Pai** (4NM19CS088) student of "NMAMIT, Nitte", has successfully completed internship from April – 2022 to August – 2022 at **Aavishk Sustainable Solutions Pvt Ltd**. The assigned project was on **Encryption**. His performance was satisfactory, and he was regular in attendance for the online sessions.

Thanks & Regards

Manoj Kumar P S
(CO – FOUNDER)

ACKNOWLEDGEMENT

I take this opportunity to express my heartfelt gratitude and appreciation to all those who provided me the support and encouragement to complete these projects. Without their contributions, inputs and suggestions, I would not have succeeded in developing the idea and completing the project. I record my indebtedness to AAVISHK SUSTAINABLE SOLUTIONS PVT LTD. for giving me a platform to learn during my internship.

My heartfelt thanks to my esteemed guide and mentor**, Mr. Sahil Bhanastarkar** from AAVISHK SUSTAINABLE SOLUTIONS PVT LTD., for his valuable advice, endless support and motivation, constantly throughout.

I would like to thank **Dr. Niranjan Chiplunkar**, Principal, NMAMIT and the Department of Computer Science and Engineering for their consistent support and providing me this opportunity to do the internship.

I would like to thank **Dr. Jyothi Shetty**, Head of Department of Computer Science and Engineering for their constant support and providing me this opportunity to do the internship.

I would like to thank my Guide **Ms. Ankitha A Nayak**, Assistant Professor Gd-II, Department of CSE for all the support and guidance.

I would like to thank AAVISHK SUSTAINABLE SOLUTIONS PVT LTD. for providing me with necessary facilities for carrying out the work and also thank all the technical and non-technical staff whose support motivated me to complete the internship.

TABLE OF CONTENTS

CONTENT **PAGE NUMBER**

LIST OF FIGURES

1. ABSTRACT

Aavishk Sustainable Solutions Pvt Ltd. let students of NMAMIT experience industry standards right in the college by providing internship after 3 rounds of interviews. This internship is approved by the college for partial requirements for the award of degree of Bachelor of Engineering in Computer Science & Engineering at NMAM Institute of Technology, Nitte.

I have done my internship on Web Development using VS Code which helped me to understand the concepts of cryptography because the project was based on encryption and learnt about how, why and where to use them.

The objective of the internship was to develop a web framework which allows the user to encrypt and decrypt text, images and files using various techniques and individually to get a firm grasp on developing website and explore the different features of VS Code.

The training focused heavily on node.js, ejs, npm install packages, concepts of cryptography, various encryption techniques, the usage of it. Also we tried understanding the various benefits of encryption for Aavishk Sustainable Solutions Pvt Ltd.

2. INTRODUCTION TO THE INDUSTRY

Aavishk Sustainable Solutions Pvt Ltd. is a B2B channel commerce and engagement platform for Brands, Dealers and Distributors. Their solution offers partners tools to sell online, manage remote businesses and make the most with business-friendly rewards. The all-in-one platform helps brands manage their network of channel commerce and make data-driven decisions with valuable insights.

The company offers tools to sell online, manage remote businesses with order and inventory management, product management, payments, reporting, and analytics, and give business rewards, enabling brands, dealers, and distributors to organize their network of channel partners and equip them to conduct remote sales.

Headquartered in Bangalore, our product helps businesses stay relevant in the new digital era, capitalize on a growing market and conduct business on-the-go.

3. DETAILS OF THE TRAINING UNDERGONE

3.1 Text Encryption and Decryption

Figure 3.1.1 Landing Page

Encrypt-O-Decrypt is a web framework designed using Node.js, Express.js, EJS, HTML, CSS for text encryption and decryption, image encryption and decryption, file encryption and decryption.

The landing page shown in figure 3.1.1 is the page that the user is able to see when the website loads for the first time. It gives the users the option for encrypting and decrypting the text, image and file. The page consists of 3 buttons namely Text Encryption, Image Encryption and File Encryption and on clicking it the user is taken to the respective web page where he/she would be able to encrypt and decrypt.

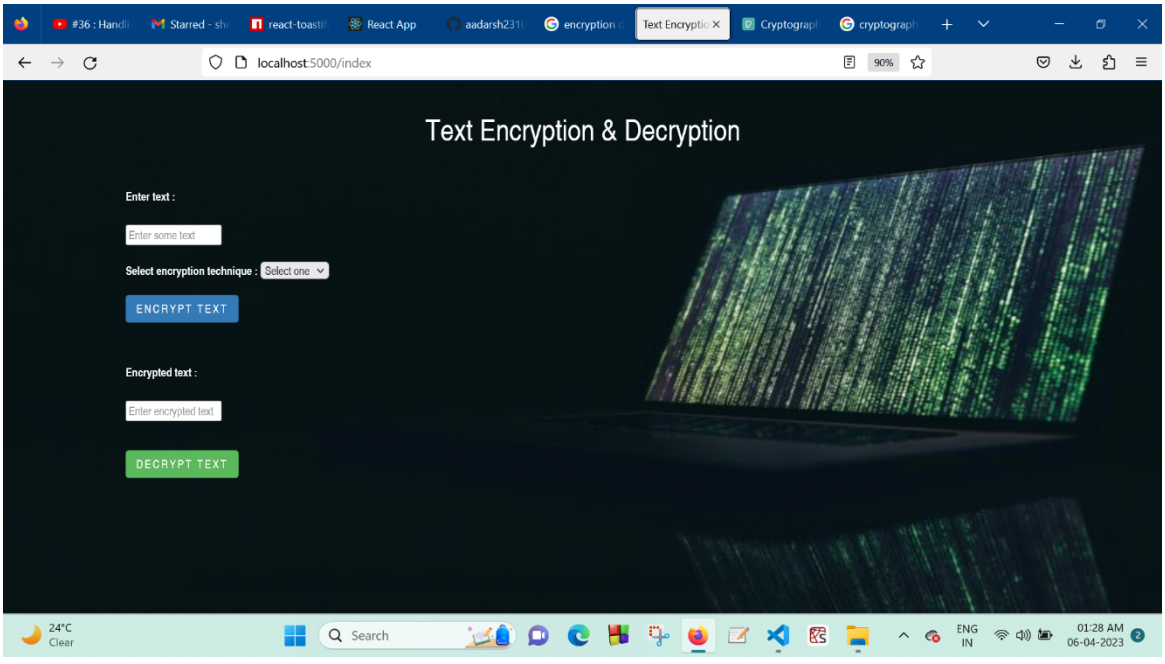

Figure 3.1.2 Text Encryption and Decryption

Text Encryption is the process of converting human-readable plaintext to incomprehensible text, also known as ciphertext. Text encryption ensures that the sender and the intended recipient are the only parties that can read a message's content.

RSA, AES and TDES are the algorithms we have used in our project. Plain text is encrypted using an encryption algorithm and an encryption key. Here the information is converted into secret code that hides the information's true meaning.

The web page consisted of 2 input fields, one to input the plaintext and latter field to input the ciphertext which is to be decrypted. It also consists of a dropdown option to select encryption technique. There are 2 buttons for encryption and decryption thereby clicking it leads to encryption and decryption of the text. The web page looks as shown in Figure 3.1.2.

3.2 Image Encryption and Decryption

Image Encryption is the process of encoding secret image with the help of some encryption algorithm in such a way that unauthorized users cannot access it. Image encryption has applications in internet communication, multimedia systems, medical imaging, telemedicine, military communication etc.

Triple DES (TDES) is the algorithm that is being implemented in our project. We encode the Image to Base64 code using TDES and then the Base64 code is later decoded and original image is obtained.

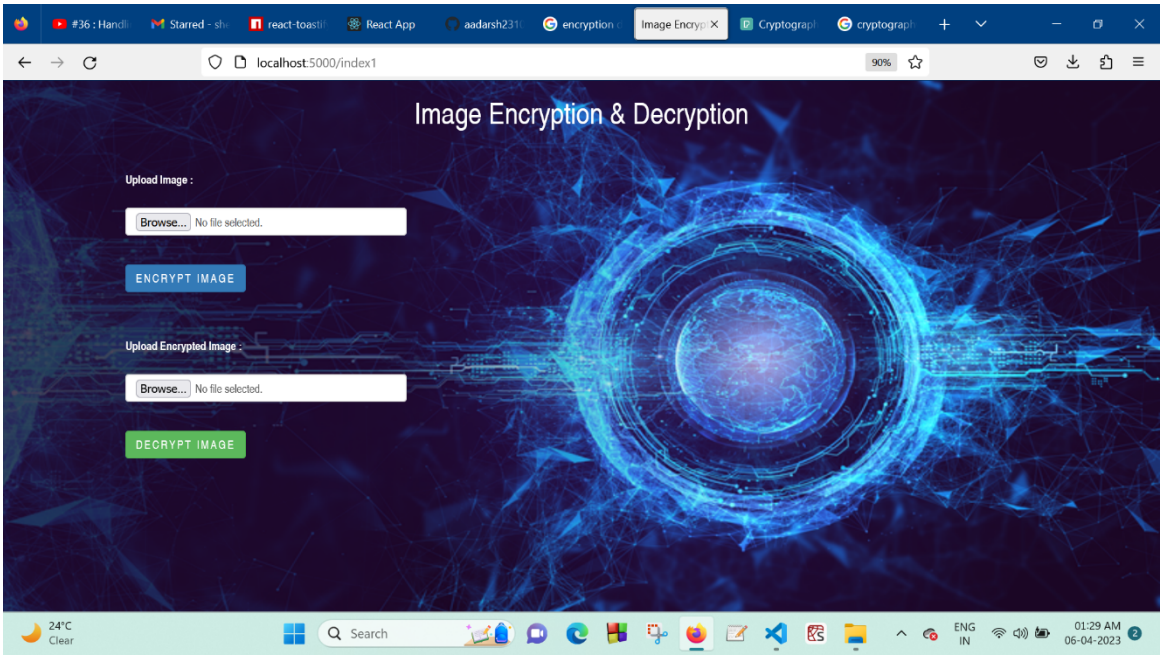

Figure 3.2.1 Image Encryption and Decryption

The web page consisted of 2 upload fields, one for upload the image and latter field to upload the Base64 code file which is to be decrypted. It also consists of 2 buttons for encryption and decryption thereby clicking it leads to encryption and decryption of the uploaded image. The web page looks as shown in Figure 3.3.1.

IMAGE ENCRYPTION TECHNIQUES –

Below are some of the best image encryption techniques :

1. Modified AES

The Advanced Encryption Standard (AES) is used as a standard by the U.S. government and various organizations. It is highly efficient in its basic 128-bit form and uses 192 and 256-bit keys for some robust encryption. AES is hailed as more effective than its predecessors such as Triple DES as it uses longer and more complex keys. The decryption is fast and finds applications in firewalls, routers or any other application that uses encryption. It is considered impervious to any attack except brute force that can try to decipher all the 128, 192 or 256-bit encryptions. It is thought to become the standard in the private sector soon as well. Modified AES is a modified AES algorithm. It is formed by the AES algorithm and a key stream generator. The latter has two different forms; (i) A5/1 key stream generator and (ii) W7 key stream generator.

2. Triple DES

Triple DES was designed as a successor to the once extensively used Data Encryption Standard (DES) algorithm. This symmetric-key method of data encryption was made obsolete by the hackers who constantly exploited its vulnerabilities. The algorithm uses a 56-bit individual key with the total key length adding up to 168 bits. However, since it is consecutive encryption, there is a middle-level vulnerability that decreases its protection to the level of a 112-bit key. Because of the complexity in the way it works, the Triple DES encryption is slower, but still, its effectiveness is good enough to keep it as one of the approved data encryption algorithms till 2030. It is also slowly phased out and used for its dependability in financial services and other industries as a hardware encryption solution.

3. RSA

The Rivest-Shamir-Adleman (RSA) is established as the standard public-key encryption algorithm. It is asymmetric because it has a public and a private key that encrypts data being sent and received. The encryption is starting on the RSA algorithm with the selection of two large prime numbers, along with an auxiliary value, as the public key. The prime numbers are keep in secret. The public key is used to encrypt a message, and private key is used to decrypt a message or information. Its scrambling level takes far too much time for any attackers to break and keeps communication quite secure. The keys for the RSA algorithms are generated by multiplying the large prime number and creating a modulus. Since the numbers involved are large, it makes RSA much safer than DES. While the Triple-DES works with keys equivalent to 112 bits, the RSA keys are 1024 to 2048 bits long. However, the 2048-bit keys are recommended by the government and IT industry.

4. Chaotic System

The term chaotic comes from “chaos” meaning confusion. It refers to a state that does not have a deterministic behavior and is a complex system that shows sensitivity towards initial conditions. Techniques focused on chaotic systems was studied and analyzed extensively in the recent years and because of its reduced mathematical complexity and better safety, this scheme is becoming influential. The encryption comprises of two components: confusion phase and diffusion phase. In confusion phase, the original or plain RGB image is partitioned into three color channels red, green and blue after that block scrambling is carried over where the image is split into blocks of sixteen. With the resultant, arnold cat map is performed to shuffle the pixels of the color image. Row-Column wise scrambling is conducted after implementing the arnold cat map.

5. BlowFish

Developed in 1993, the Blowfish encryption algorithm is an alternative for Data Encryption Standard (DES). The developer placed the protocol to the public to make it readily available for any interested user compared to DES, it is substantially faster and offers better encryption security. It is an asymmetric type of encryption protocol: uses a single key for both encryption and decryption. It is a significantly fast operation because it involves a relatively small number of rounds as well as its clarity of functionality. Nevertheless, its key-scheduling consumes a lot of time, although it has an upper hand when it comes to protecting brute-force threats. Also, its 64-bit block length (size) is rather small making it endangered by birthday attacks compared to AES whose block size is 128 bits and above.

6. Image Encryption using Affine Transform and XOR Operation

It is a symmetric key encryption technique that first scrambles the locations of pixels using four 8-bit sub keys and then encrypt the pixel values by XOR the selected 9-bit key. The scrambling operation is done using Arnold transformation cipher techniques that breaks the correlations of the neighboring pixels and make image unidentifiable. The XOR operation then changes the pixel values making the image very meaningless.

7. TwoFish

This form of the encryption algorithm is a symmetric key block cipher which is characterized by 128-bit block size and whose keys' size can run up to 256 bits. This protocol uses one key for encryption and decryption. It is a fast and flexible standard for eight-bit and thirty two-bit CPUs, and small smart cards. The protocol works exemplarily in hardware and has numerous functionality commutations between the speed of encryption and setup time making it distinctive.

3.3 File Encryption and Decryption

File Encryption is the process of encoding files, including the sensitive data they contain, in order to send them securely. File encryption sees to it that our files are not at risk, also ensuring that the security is not compromised.

RSA is the algorithm that is being implemented for file encryption. Here we encode the file in .pdf format to Base64 code using RSA and then the Base64 code is later decoded and the original file is obtained.

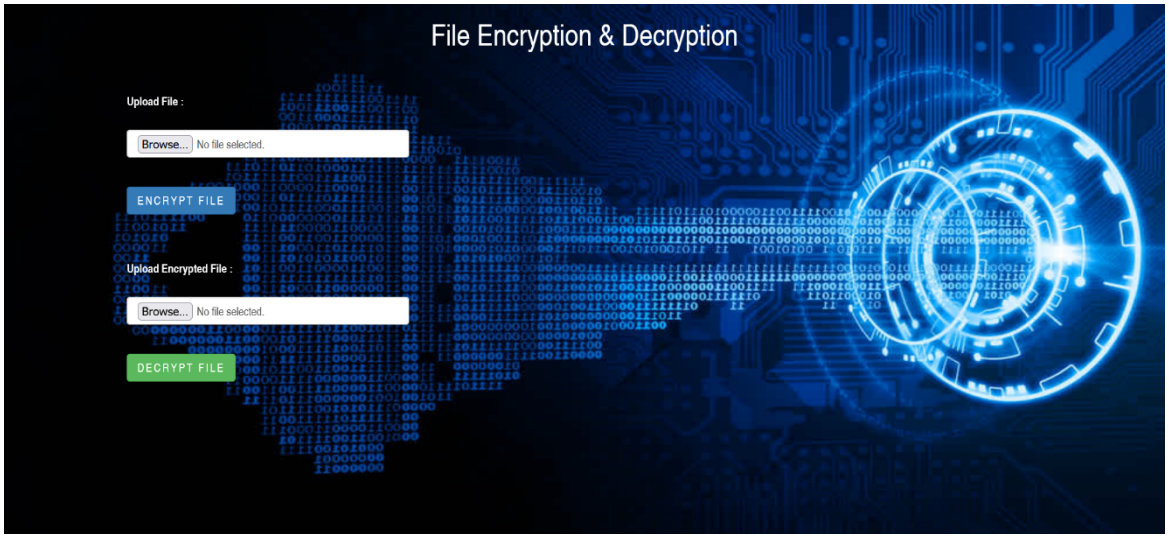

Figure 3.3.1 File Encryption and Decryption

The web page consisted of 2 upload fields, one for upload the file to be encrypted and latter field to upload the Base64 code file which is to be decrypted. It also consists of 2 buttons for encryption and decryption respectively thereby clicking it leads to encryption and decryption of the uploaded file. The web page looks as shown in Figure 3.3.1.

FILE ENCRYPTION TECHNIQUES -

Below are some of the best file encryption techniques :

1. Advanced Encryption Standard Crypt

AES Crypt is a file encryption software available on several operating systems that uses the industry standard Advanced Encryption Standard (AES) to easily and securely encrypt files. Using a powerful 256-bit encryption algorithm, AES Crypt can safely secure most sensitive files. perfect solution for those who wish to backup information and store that data at a bank, in a cloud-based storage service, and any place where sensitive files might be accessible by someone else.

2. Rivest-Shamir-Adleman (RSA)

Rivest-Shamir-Adleman is an asymmetric encryption algorithm that is based on the factorization of the product of two large prime numbers. Only someone with the knowledge of these numbers will be able to decode the message successfully. RSA is often used when transmitting data between two separate endpoints (e.g., web connections), but works slowly when large volumes of data need to be encrypted.

3. DES-X

The reason for the introduction of the DES-X was an attempt to increase the security of the original DES algorithm. The proposed solution with DEX-X was to use two more 64-bit keys which would be applied to make it harder for an attacker to guess the key of the DES algorithm. Basically, the first additional key is XORed to the plain text which is then encrypted with DES. The second additional key is XORed to the resulting cipher.

4. Triple DES (Data Encryption Standard)

Triple DES is a symmetric encryption and an advanced form of the DES method that encrypts blocks of data using a 56-bit key. Triple DES applies the DES cipher algorithm three times to each data block. Triple DES is commonly used to encrypt ATM PINs and UNIX passwords.

5. Twofish

Twofish is a license-free encryption method that ciphers data blocks of 128 bits. It's considered the successor to the 64-bit Blowfish encryption method and more versatile than its specialized successor, Threefish. Twofish always encrypts data in 16 rounds regardless of the key size. Though it works slower than AES, the Twofish encryption method continues to be used by some file and folder encryption software solutions.

6. Open SSL Tool

OpenSSL is an amazing tool that does a variety of tasks, including encrypting files.

Step 1: Generate key pairs

Before you can encrypt files, you need to generate a pair of keys. You will also need a passphrase, which you must use whenever you use OpenSSL, so make sure to remember it.

Step 2: Extract the public keys

Remember, the public key is the one you can freely share with others, whereas you must keep your private key secret. So, Alice must extract her public key and save it to a file using the commands.

Step 3: Exchange public keys

These public keys are not much use until they exchange them with each other. Several methods are available for sharing public keys, including copying the keys to each other's workstations using the scp command.

Step 4: Exchange encrypted messages with a public key

To encrypt this secret message, one needs to use the openssls -encrypt command, providing three inputs to the tool:

1. The name of the file that contains the secret message
2. public key (file)
3. The name of a file where the encrypted message will be stored

After encryption, the original file is still viewable, whereas the newly created encrypted file looks gibberish on the screen. You can be assured that the secret message has been encrypted.

Step 5: Decrypt the file using a private key

Using the -decrypt command-line argument providing the following information to the utility:

1. The encrypted file (which he got from sender).
2. own private key.
3. A file name to save the decrypted output to via redirection.

4. CONCLUSION

It was a great experience being a part of Aavishk Sustainable Solutions Pvt Ltd. All in all, got to learn a lot from this internship. Amount of knowledge that we got is truly a blessing. Got basic knowledge on how corporate world works. It also introduced to work in the groups and brainstorm our mind. It was a friendly atmosphere where each of us helped one another. Time management skill is the key highlight of this internship. I came out more experienced as software developer.

The 4 months of internship also gave me insight into the cryptography concepts, the real-time applications of it and also got an idea on how actually an industry works and technologies that are helpful in recent times.

I have come out of internship more confident in myself and would like thank AAVISHK SUSTAINABLE SOLUTIONS PVT LTD for letting me into their platform for this amazing experience.

5. REFERENCES

1. https://github.com/K-Sheshadri-Pai/Crypto_Avysh
2. https://www.npmjs.com/package/cryptography
3. https://www.w3schools.com/nodejs/ref_crypto.asp
4. https://www.avysh.com