A Project Submitted to

Vivekanand College, Kolhapur (Empowered Autonomous)

VIVEKANAND COLLEGE

KOLHAPUR

Affiliated to

Shivaji University, Kolhapur

For the Degree of Bachelor of Science

In Mathematics

By

Name: Neha Rajesh Shinde

Roll No: 8302

Exam Seat No:600402

B.Sc. III (Mathematics)

Year: 2023-24

Under the Guidance of

Ms. P.P. Kulkarni

(Assistant Professor , Department of Mathematics)

Vivekanand College (Empowered Autonomous),Kolhapur

Dissemination Of Education For Knowledge ,Science & culture"

Shikshanmaharshi Dr. Bapuji Salunkhe

Shri. Swami Vivekanand Shikshan Sanstha,
Kolhapur

Vivekanand College, Kolhapur
(Empowered Autonomous)

DEPARTMENT OF MATHEMATICS

Certificate

This is to certify that Neha Rajesh Shinde has successfully completed the project work on topic "Cryptograhy" towards the partial fulfilment for the course of Bachelor of Science (Mathematics) work of Vivekanand College, Kolhapur (Empowered Autonomous) affiliated to Shivaji University, Kolhapur during the academic year 2023-2024.

Place: Kolhapur

Date: 23|03|2024

Examiner

Mr. S.P. Thorat
Head Dept. of Mathematics

HEAD
DEPARTMENT OF MATHEMATICS
VIVEKANAND COLLEGE, KOLHAPUR
(EMPOWERED AUTONOMOUS)

DECLARATION

I, Miss. Shinde Neha Rajesh solemnly declare that this project report titled "Cryptography" is an original piece of work carried out by me under the guidance of Ms. P.P Kulkarni. The information and ideas presented herein are my own and have been gathered from authentic sources to the best of my knowledge.

All sources used in this report have been duly acknowledged and referenced. Any external contributions to this work are clearly cited in the bibliography section. I have not submitted this report, or any part thereof, for any academic or professional qualification previously.

I further declare that this work has not been published elsewhere in any form and is not under consideration for publication elsewhere.

Date: 21/03/2024

ACKNOWLEDGMENT

I would like to express my sincere gratitude and appreciation to my mentor P.P Kulkarni for their invaluable support, guidance, and expertise throughout the completion of this project. Their contribution played a crucial role in achieving the goals set forth in this report.

I also thank **Dr. R.R Kumbhar** (Principal, Vivekanand College,Kolhapur (Empowered Autonomous)) , **Prof. S.P Thorat** (HoD Mathematics, Vivekanand College,Kolhapur, (Empowered Autonomous)), The whole Department of Mathematics of Vivekanand College, Kolhapur their unwavering encouragement, belief in my capabilities, and the environment of academic excellence fostered within The Vivekanand College,Kolhapur have played an instrumental role in shaping my academic journey. Both of their contributions, whether through academic insights, institutional resources, or mentorship, have significantly enriched the trajectory of my research endeavor. Moreover I am also thankful non teaching staff Mr. Dilip Birnale And Sagar Suryavanshi Sir.

Finally, I am grateful to department of Mathematics for lending me this opportunity that made this project possible.

CONTENTS

Aims and Objectives 7- 8

Introduction..9-10

Theoretical framework of the topic 11-12

Chapter 1: CRYPTOGRAPHY:..13-17

1.1 What is cryptography
1.2 Importance and relevance of cryptography
1.3 Why do we need cryptography
1.4 Importance of cryptography
1.5 Goals of cryptography

Chapter 2: TYPES OF CRYPTOGRAPHY...............................18

2.1. Symmetric Encryption

2.2. Asymmetric Encryption

2.3. Hash Functions

Chapter 3: Feasible use of cryptography................................19-29

3.1 Electronic pollbooks

3.1.1 What is AES encryption and how does it work?

3.1.2 Public Key Encryption

3.1.3 Digital Signatures

3.1.4 Sorting the votes and removing digital signatures

3.1.5 Decryption and Final count

3.1.6 Verifying the vote

Chapter 4 : METHODOLOGY 30-32

4.1 Digital signature and RSA digital signature

4.2 The mechanism behind the RSA algorithm

4.2.1 Generating public key

4.2.2 Generating private key

4.3 The implementation of the RSA algorithm(python)

Chapter 5 : ADVANTAGES of Cryptography……………………..……33

Conclusion……………………………………...…………………...34

References……………………………………..……………...……35

AIMS AND OBJECTIVES

Aims:

1. Comprehending Encryption Techniques: The project's goal is to investigate the different cryptography-related encryption techniques, including hashing and symmetric and asymmetric encryption.

2. Implement secure communication techniques:

Develop programs or algorithms that enable secure communicaton to protect against malicious or unwanted information.

3.Improving information security: Use cryptography technology to research and recommend ways to improve information security in various industries (banking, healthcare, etc.).

4.Application: Demonstrate that encryption concepts can protect sensitive data using real-world situations.

Objectives:

1. Learn about Cryptographic Algorithms: Examine and comprehend the underlying theories of several cryptographic algorithms, such as RSA, AES, DES, and so on.

2. Algorithm Implementation: Use a few chosen encryption algorithms to encrypt and decode data while demonstrating their security features and usefulness.

3. Security Analysis: Evaluate the selected encryption techniques in-depth, looking for any potential weak points and suggesting fixes to reduce risks.

4. Performance Evaluation: To ascertain the practicality of encryption systems, assess their performance in terms of speed, resource consumption, and scalability.

5. Prototype Development: Construct a simulation or prototype that illustrates how cryptography is used in a particular setting (secure messaging, data storage, etc.).

6. Documentation and Presentation: Put together a thorough report and presentation that highlights the project's methods, conclusions, and ramifications for more study or real-world application.

INTRODUCTION

Cryptography plays the duty of a sentinel protecting our digital interactions at a time when information is a currency and data security is a fundamental requirement. Beyond simple encryption, cryptography—the art and science of secure communication—has evolved into the cornerstone of contemporary cyber security, guaranteeing authenticity, secrecy, and integrity in our digital age.

The goal of this project is to investigate the many facets of cryptography, including its historical foundations, developing techniques, and modern applications. This programme intends to bring forward the different uses of data and to demystify the mysterious methods in which it is protected, decrypted, and used by breaking down the complexity of cryptographic algorithms.

The primary objective of this project is to both clarify the basic concepts of cryptography and examine its applications in protecting confidential data in a variety of contexts. Each component is essential to strengthening our digital infrastructure, whether it is the strong hashing algorithms protecting data integrity or the asymmetric encryption approaches protecting financial transactions.

This initiative aims to clarify both the theoretical ideas and real-world applications of cryptography through its investigation. It hopes to further knowledge of how cryptography protects our digital life and the critical role it plays in thwarting possible security threats by doing this.

At the completion of this project, it is hoped that a thorough grasp of the workings and applications of cryptography will be attained, opening the door to well-informed debates and new developments in this dynamic area.

THEORETICAL FRAMEWORK OF TOPIC

Establishing the fundamental ideas, guiding principles, and pertinent theories from previous research is a necessary step in developing a theoretical framework for a cryptography project.

1. Synopsis of Cryptography:

Describe the idea of cryptography, its development throughout time, and its importance for data and communication security.

2. Essential Ideas

- Encryption and Decryption: Describe the fundamental steps involved in transforming plaintext into ciphertext and the other way around.

Important Ideas: Describe the significance of keys (both symmetric and asymmetric) in the encryption and decryption procedures.

- Security Goals: Talk about the four main goals of cryptography: non-repudiation, integrity, secrecy, and authentication.

3. Cryptographic Algorithm Types:

- Symmetric Encryption: Explain the operation of symmetric key algorithms such as AES and DES.

- Asymmetric Encryption: Describe the special characteristics of asymmetric key methods such as RSA and ECC.

- Hash Functions: Talk about how hash functions protect the integrity of data.

4. Cryptography Applications:

- Secure Communication: Describe the role that cryptography plays in protocols for secure communication such as SSH, TLS/SSL, etc.

- Data Security: Talk about how cryptography helps protect data both in transit and at rest (using disc encryption, for example).

5. Cryptanalysis:

Talk about several cryptographic assaults, such as specific cypher text attacks, known plaintext, and brute force attacks, as well as flaws in cryptographic systems.

- Quantum Cryptography: Explain the idea behind it and how it could affect more established encryption techniques.

6. Legal and Ethical Implications:

Compliance and Regulations: Talk about the legal frameworks that restrict cryptography, such as export rules and privacy regulations.

- Ethical Considerations: Examine moral conundrums surrounding cryptography, such as juggling concerns about national security with private rights.

7. Present Patterns and Prospective Routes:

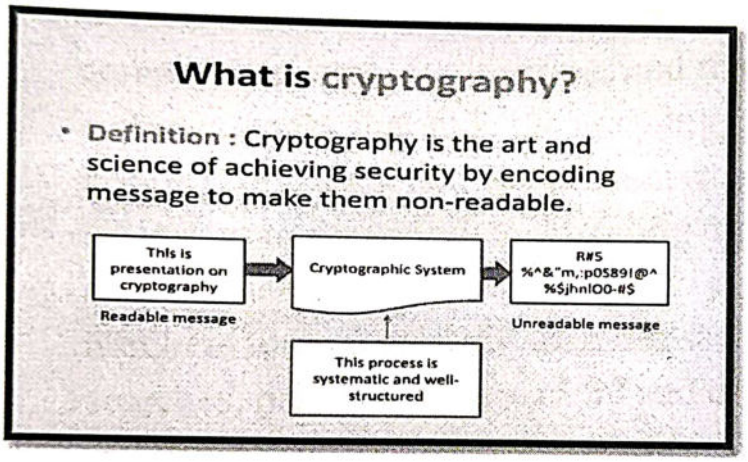
- Post-Quantum Cryptography: Talk about the latest advancements and ongoing research in this field.

- Blockchain and Cryptography: Examine how blockchain technology and cryptography interact.

Chapter 1: CRYPTOGRAPHY

1.1 What is Cryptography?

The practice of hiding or encoding a message so that only the intended recipient can read it is called cryptography. The application of cryptography to encode information has been used for thousands of years. Today, it is still used in e-commerce, bank cards and computer passwords. Accessing and decrypting data is done using modern encryption techniques, including ciphers and algorithms such as 128-bit and 256-bit encryption keys. Modern encryption systems such as Advanced Encryption Standard (AES) are considered virtually unbreakable. Message encoding is used to ensure that the message can only be read and processed by its recipient and is a hot topic in cryptography. Cryptography is another name for cybersecurity techniques that combine computer science, engineering, and mathematics to create complex codes that hide the meaning of a word. Although it has its roots in ancient Egyptian hieroglyphs, cryptography is important to prevent unauthorized reading when they are in circulation. It uses mathematical techniques and techniques to turn one word into several words to protect credit cards, emails, online searches, personal information and digital signatures. The practice of storing or concealing information so that only the



What is cryptography?

- Definition : Cryptography is the art and science of achieving security by encoding message to make them non-readable.

This is presentation on cryptography

Readable message

Cryptographic System

R#S %^&"m,:p05891@^ %$jhnlOO-#S

Unreadable message

This process is systematic and well-structured intended recipient can read it is called cryptography. The application of cryptography to encode information has been used for thousands of years. Today, it is still used in e-commerce, bank cards and computer passwords. Accessing and decrypting data is done using modern 'encryption techniques, including ciphers and algorithms such as 128-bit and 256-bit encryption keys. Modern encryption systems such as Advanced Encryption Standard (AES) are considered virtually unbreakable. Message encoding is used to ensure that the message can only be read and processed by its recipient and is a hot topic in cryptography. Cryptography is another name for cybersecurity techniques that combine computer science, engineering, and mathematics to create complex codes that hide the meaning of a word. Although it has its roots in ancient Egyptian hieroglyphs, cryptography is important to prevent illegal reading during transmission. It uses mathematics and techniques to convert text into multiple numbers to protect credit card transactions, emails, online searches, personal information, and digital signatures.

1.2 Importance and relevance of cryptography in modern world.

Technology has made our lives easier, but it has also made our personal information more vulnerable. Computers are designed to follow your instructions without making mistakes, but sometimes you don't want them to reveal confidential information. Most of us talk about privacy in our daily lives. Whether it's about the information available or whether your digital footprint is being tracked, the answer to this question has never been clearer. Due to increased restrictions, there are concerns about cyber attacks and privacy violations. This is what cryptography does. This is the science of hiding things. It takes data and encrypts it so that the computer cannot decrypt it without permission. Let's take an example where you need to send some confidential information to other people around the world. You can't send the message to the recipient because he or she is halfway around the world, and you don't want anyone to read or modify the message because it contains sensitive information. When you send a message, there are many people responsible for managing the communication between you and the recipient. Communications can be mistaken or fall into the wrong hands, giving them access to private information. If the intermediary acts unfairly, he has two options: He can either keep the information to himself, or listen carefully and allow the communication to continue. Therefore, it is recommended to encrypt data when sending sensitive or private messages. Communications can be accessed using encryption technology that will prevent someone from intercepting it and determining its content. Encryption is crucial in today's digital age, where a word can be sent to anyone in the world with one click. Thanks to the advent of digital encryption, we are approaching a time when privacy will change forever, at least when it comes to digital communications. Access your private messages in a few clicks from your smartphone. In the digital age, encryption technology is often used for purposes other than encrypting private information. Businesses are increasingly using it to protect their intellectual property and secure their communications.

1.3 Why do we need Cryptography?

Everything we do online today is monitored and recorded by many companies, including banks, credit card companies, Google, Facebook and more. Most people are not aware of the information available on the internet. Never before have we seen so much data collected, analyzed and stored. Moreover, working power and computer power are increasing simultaneously, allowing companies to collect, analyze and store more information. Many consumers are unaware of the many new security threats that come with all this additional information. This is a particular problem in the context of large amounts of data. Big data has great consequences but also dangers. It is generally believed that hackers pose an additional risk to individuals and businesses. They are always looking for new ways to achieve their goals. As a result, cyber attacks are on the rise as hackers try to bypass the network or steal data. This means that attacks can be carried out by more motivated individuals and groups. By 2022, the average cost of a data breach will reach $4.35 million. It is estimated that 71% of data crimes are money-related and cybercrime will cost the world economy $10.5 trillion annually by 2025. Cryptography is more important than ever As cyber attacks become more frequent, organizations and individuals can protect their information. and communications resulting from unauthorized access.

1.4 Importance of Cryptography:

Encryption is the practice of modifying data so that only the intended recipient can decrypt it. Without encryption, privacy and confidentiality would not be possible in the digital world. Everything can be easily stolen. The importance of cryptography has increased over time, especially considering the increase in cyber attacks. It is important for network security as it prevents theft, unauthorized access and data loss. It also helps protect the privacy of Internet users. Businesses and individuals can increase their security and privacy by encrypting sensitive data. Another feature it provides allows users to verify that the messages they send or receive come from the intended source. "Encryption" means secret, "graphics" means written. Encryption technology converts information (text) into a secret form that can only be read by those who need the key. The information is then placed in a secure database and encrypted. In fact, the foundation of all online interactions is digital trust, and most people who use encryption regularly don't even know it.

1.5 Purpose of Cryptography: Cryptography uses mathematical techniques and methods to encrypt and decrypt information to ensure that only authorized users can access it. The two main goals of encryption are user authentication and protection of the accuracy, integrity and confidentiality of information. Another basis of the cryptographic system that allows users to verify information and prove themselves is the digital signature.

Chapter 2: TYPES OF CRYPTOGRAPHY

Cryptography is a field of mathematics concerned with information and communications security. In the narrow sense, it is the practice of converting readable data into an unreadable format.

2.1 Key encryption (symmetric encryption): In symmetric encryption, a key is used for data encryption and decryption. This means that data is encrypted and decrypted using the same key. It is one of the most secure forms of coding and is suitable for many situations. Symmetric encryption is sometimes called secret key encryption because the sender and receiver must share the same key to complete the encryption decision. It is very secure because it is impossible for someone without the key to decipher the information.

2.2 Asymmetric Encryption : In this method, two keys are used to encrypt and decrypt data. The encryption process uses the recipient's public key, while the decryption process uses the recipient's private key. Private keys and public keys are different. Only the recipient of the plan knows his private key, so even if anyone can access the public key, he or she is the only one who can decipher it. RSA algorithm is the most commonly used asymmetric key encryption algorithm.

2.3 Hash function : This algorithm does not use any keys. Since the fixed-length hash value is calculated as text, it is difficult to reconstruct the contents of plaintext. Hash functions are often used to encrypt passwords in operating systems.

Chapter 3: FEASIBLE USE OF CRYPTOGRAPHY

3.1 Electronic Poll Book:

The electronic poll book is the first electronic voting machine that voters may encounter at the polling station. These are three-ring files containing digitally altered voter registration documents. Election officials can search for voters, identify them, and take additional steps to ensure they vote validly using an electronic ballot. These voting books contain sensitive information that could be compromised in a variety of ways if disclosed. If the electronic voting book captures the order in which people vote, it can be used to remove anonymous votes. The attacker simply matches the voting data with the data from the computerized ballot to determine how each voter voted. This could lead to voter intimidation. Electronic voting books store a lot of voting data; therefore, it must use a protocol such as AES to access data in transit and data at rest. In addition to protecting voter privacy, this also prevents hackers from controlling data or otherwise affecting the system. Electronic voting requires the use of a cashier's check to verify its legitimacy prior to use. If your computer's hash matches its hash value, it is generally accepted that the software is safe to use and genuine.

3.1.1 What is AES encryption and how does it work?

The message you want to encrypt (called plaintext) is first divided into blocks according to the encryption process. Since the block size of AES is 128 bits, the data is divided into 4x4 lines of 16 bytes each (16x8 = 128 bytes). If your message is "Please Buy me some potato chips," the first block will look like this:

b	m	o	p
u	e	m	o
y		e	t
	s		a

KEY EXPANSION:

For each different type of encryption, many new keys are created using the original key in a process called key expansion. Rijndael's main work is used to provide these new 128-bit round keys, which are a simple and easy way to create new key encryption. If the first key is "key boring 1":

k			i
e	a	b	n
y	r	o	g
s	e	r	1

Then each of the new keys might look something like this once Rijndael's key schedule has been used:

14	29	1h	s5
h9	9f	st	9f
gt	2h	hq	73
ks	Dj	df	hb

When AES encryption is really used, each of these keys is produced from an organised procedure, even if they appear to be random characters (the example above is fictitious).

ADD ROUND KEY:

In this step, because it is the first round, our initial key is added to the block of our message:

b	m	o	p
u	e	m	o
y		e	t
	s		a

+

k			i
e	a	b	n
y	r	o	g
s	e	r	l

An XOR cypher, an additive encryption method, is used to accomplish this. Even if it appears that these can't be added together, remember that this is really done in binary. The characters serve only as a stand-in to help with comprehension. Assume for the moment that the outcome of this mathematical operation is:

h3	jd	zu	7s
s8	7d	26	2n

dj	4b	9d	9c
74	el	2h	hg

SUBSTITUTE BYTES:

Every byte is replaced in this stage in accordance with a preset table. This resembles the example given at the beginning of the article in that it codes the sentence by replacing each letter in the sentence with the letter that follows it in the alphabet (hello becomes ifmmp).

This system is a little bit more intricate, however it's not always logical. Alternatively, the algorithm can seek up a pre-established table that states, for instance, that h3 becomes jb, s8 becomes 9f, dj becomes 62, and so on. Let us assume that following this stage, the predefined table provides us with:

jb	n3	kf	n2
9f	jj	1h	js
74	wh	0d	18
hs	17	d6	px

MIX COLOUMS

It's a little difficult to describe this stage. Let's simply suppose that each column has a mathematical equation applied to it in order to further disperse it, to exclude much of the arithmetic and make things simpler. Assume that this is the outcome of the procedure:

ls	j4	2n	ma

83	28	ke	9f
9w	xm	31	m4
5b	a9	cj	ps

ADD ROUND KEY AGAIN:

Do you recall the round keys we created at the beginning utilising Rijndael's key schedule and our original key? This is the point at which we put them to use. We apply the first round key we generated to the outcome of our mixed columns:

ls	j4	2n	ma
83	28	ke	9f
9w	xm	31	m4
5b	a9	cj	ps

+

14	29	1h	s5
h9	9f	st	9f
gt	2h	hq	73
ks	dj	df	hb

Let’s say that this operation gives us the following result:

9d	5b	28	sf

ls	df	hf	3b
9t	28	hp	8f
62	7d	15	ah

If you think so, we are still a long way from it. After the last set of keys is added, the process returns to the bit-tuple key step, where each value is updated according to the specified table. When you're done, go back to moving lines and move each line one, two, or three spaces to the left. Then run the balance line again. Another round key was added later. And it's not over yet. As mentioned at the beginning, the AES size is 128, 192 or 256 bits. There are nine rounds when using a 128-bit key. 11 when a 192-bit key is used. 13 when a 256-bit key is used. Thus, the data is modified at each stage, up to thirteen times per stage, as it passes through the byte conversion, row conversion, column shuffling, and key stages. Once the user's vote is verified, the vote is approved by the voters. Traditional vote book or electronic vote book. Voters can obtain tokens or smart cards to use electronic voting machines (DRE) directly at polling stations, allowing them to vote on the device. These cards usually have encryption keys on them that tell the computer that the holder has the right to vote. Similar to electronic voting software, DRE software requires legal verification before use. The check must be successful to ensure that the number has not been changed or tampered with. If the hashes match, the program will be safe to use.

STORAGE:

Votes that have been cast should be encrypted and kept on the DRM for storage. This makes it far more difficult for attackers to change votes and stops them from being viewed. Regretfully, during storage, votes aren't always encrypted. In some instances, researchers have even bought vintage voting machines from eBay and looked at the results of the previous election in which they were utilised. This indicates that when the election was over, the votes were still on the machine, unencrypted, and hadn't even been deleted. This is a serious breach of privacy and security.

TRANSMISSION: To stop hackers from stealing votes and changing the outcome, votes must also be encrypted while they are in route. Security protocols such as TLS are frequently utilised in transmission. This is a hybrid system that incorporates additional security elements together with symmetric techniques like AES and public-key encryption cyphers like RSA. Switzerland has started employing quantum key distribution in recent years to determine whether there is a chance that hackers may be able to intercept its encryption keys.

TABULATION: The most important aspect of the election is the outcome. Attackers could change the winner if they could figure out how to modify it covertly. In the event if foes were discovered before to the election's conclusion and the attacks were halted, a great deal of distrust would be ingrained in the system, leading many voters to doubt the election's validity. Verifying that the vote tallying equipment is running the appropriate software is crucial. This implies that in order to confirm that the code hasn't been altered, checksums are required. Additionally, these devices must be protected so that only authorized personnel can access them. Keys need to be stored securely to prevent attackers from manipulating the results.

during storage, votes aren't always encrypted. In some instances, researchers have even bought vintage voting machines from eBay and looked at the results of the previous election in which they were utilised. This indicates that when the election was over, the votes were still on the machine, unencrypted, and hadn't even been deleted. This is a serious breach of privacy and security.

TRANSMISSION: To stop hackers from stealing votes and changing the outcome, votes must also be encrypted while they are in route. Security protocols such as TLS are frequently utilised in transmission. This is a hybrid system that incorporates additional security elements together with symmetric techniques like AES and public-key encryption cyphers like RSA. Switzerland has started employing quantum key distribution in recent years to determine whether there is a chance that hackers may be able to intercept its encryption keys.

TABULATION: The most important aspect of the election is the outcome. Attackers could change the winner if they could figure out how to modify it covertly. In the event if foes were discovered before to the election's conclusion and the attacks were halted, a great deal of distrust would be ingrained in the system, leading many voters to doubt the election's validity. Verifying that the vote tallying equipment is running the appropriate software is crucial. This implies that in order to confirm that the code hasn't been altered, checksums are required. Additionally, these devices must be protected so that only authorized personnel can access them. Keys need to be stored securely to prevent attackers from manipulating the results.

Digital ID Card: The ability to sign documents using the public card and the identity of the significant partner is one of the most important. While a person's public key can be used to identify themselves, their private key can be used to create a digital signature. People download ballot papers to their laptops to vote. The USB card reader they plug in then reads their ID. They enter their PIN number to verify their identity. Voters also have the option of using a different identity system linked to their mobile phone number. They input both the number and their PIN into the programme. The voter's information is verified by the systems in both situations by cross-referencing it with the electoral register. Because an attacker would need to obtain both the voter's PIN and digital identity card, it becomes extremely difficult to cast fake ballots.

3.1.2 Public key encryption:

We can use two envelope methods to ensure the security and anonymity of voting. When a user votes on their computer and enters the voting system, random numbers are added to the database. Votes cast and numbers generated are then encrypted using a public voting key. This creates an inner envelope that conceals the voter's identity.

3.1.3 DIGITAL SIGNATURES:

Once the ballot is encrypted and placed inside the envelope, the voter's key is used to sign the ballot. The ballot is then sent to the electronic voting machine. It is protected by the TLS security protocol during transmission. When you share sensitive information online, such as when you log into your bank account or enter your password on Facebook, TLS, a model of different encryption protocols, keeps your data safe. When you visit a website that uses TLS, you will see a small green lock to the left of the URL and the website address starts with https instead of http. After that all votes are collected and scheduled. Voters' qualifications are also verified and double voting to remove unqualified votes (permitted under the Estonian system, but only the last vote is accepted against coercion).

3.1.4 SORTING THE VOTES AND REMOVING DIGITAL SIGNATURES:

After that, the voter's electoral district is used to sort the i-votes, and the digital signatures are eliminated. In doing so, the voter's identify is removed from the ballot. After then, the votes are randomly distributed across several servers in a mix network, rendering it impossible to link a vote to the voter's identity. This measure helps to avoid intimidation and preserves the vote's confidentiality.

3.1.5 DECRYPTION AND FINAL COUNT :

Following that, the shuffled votes are sent to an air-gapped server so that the encryption may be broken. Because this server isn't linked to the internet or any other networks, hackers can't virtually compromise it. Next, using the private key unique to that election, the votes are decoded.

The key is not in the hands of one individual; several election officials work together to finish the key assembly. The authorities must insert their authentication tokens into the server and then enter their PIN numbers in order to decode the vote. Because an attacker would have to compromise every official to have access, it would be more harder to interfere with the election results.

The votes are moved to an air-gapped vote counting server after they have been decrypted so that they may be promptly totaled. The election winner can be declared when the ballots have been tallied.

When combined, these techniques allow for the relatively safe and anonymous conduct of an online vote through the use of cryptography and careful organisational procedures.

3.1.6 VERIFYING THE VOTE:

A lot of individuals have doubts about voting online. Ultimately, you are unable to view the actual traffic flowing between the servers and your machine. When using a paper ballot, you physically place it in the box and put your confidence in the unbiased observers to handle the rest.

We can implement a verification mechanism that lets individuals examine their ballots and feel more at peace in order to allay their anxieties. Voter verification can only be completed using an app on a phone or tablet, even though online votes must be cast through an application on the voter's PC.

This division serves as a security precaution. If the voter's computer were used for both procedures, an attacker would only need to infiltrate one device to secretly alter the voter's vote. Both devices would need to be compromised by the attackers.

Upon finishing the voting process, a QR code appears on the user's computer screen. Using the election app on their phone or tablet, the voter may scan it. The voter may then verify that their vote was cast accurately by using the app, which will show their ballot as it was received by the server.

Cryptography is essential to the security of any electronic or online voting systems that are going to be employed.

Chapter 4: METHODOLOGY

4.1 Digital signature: The message's integrity is ensured by the digital signature system, which may also be used to identify the message's source.

RSA digital signature: The RSA digital signature technique consists of three algorithms: Key Generation, Signing, and Verification.

An asymmetric cryptography algorithm is the RSA algorithm. In actuality, asymmetric refers to the fact that it operates on both the public and private keys. As implied by the name, the private key is kept secret while the public key is distributed to everybody.

Asymmetric cryptography example:

1. A client requests data from the server by sending its public key to it, such as a browser.

2. The data is sent by the server encrypted with the client's public key.

3. After receiving this data, the client decrypts it.

Because this is asymmetric, even if someone else has the browser's public key, only the browser itself is able to decode the data. The notion! Large integers are hard to factorise, which is the foundation for the RSA concept. Two numbers make up the public key, one of which is the product of two big prime numbers. The same two prime numbers are also used to generate the private key. Therefore, the private key is compromised if the huge integer can be factorised. As a result, the key size determines the encryption strength entirely, and the strength of the encryption rises exponentially as the key size is doubled or tripled. RSA keys are normally 2048 or 1024 bits long, but experts predict that 1024-bit keys will soon be cracked. However, it appears to be an impossible feat as of yet.

4.2 The mechanism behind the RSA algorithm :

4.2.1 >> Generating Public Key:

Select two prime no's. Suppose P = 53 and Q = 59.

Now First part of the Public key : n = P*Q = 3127. We also need a small exponent say e : But e Must be An integer. Not be a factor of Φ(n).

$1 < e <$

$1 < e < \Phi(n)$ [Φ(n) is discussed below], Let us now consider it to be equal to 3. Our Public Key is made of n and e

4.2.2 >> Generating Private Key:

We need to calculate Φ(n) : Such that Φ(n) = (P-1)(Q-1) so, Φ(n) = 3016 Now calculate Private Key, d : d = (k*Φ(n) + 1) / e for some integer k For k = 2, value of d is 2011.

Now we are ready with our – Public Key (n = 3127 and e = 3) and Private Key(d = 2011) Now we will encrypt "HI": Convert letters to numbers : H = 8 and I = 9 Thus Encrypted Data c = (89e)mod n Thus our Encrypted Data comes out to be 1394 Now we will decrypt 1394 : Decrypted Data = (cd)mod n

Thus our Encrypted Data comes out to be 89 8 = H and I = 9 i.e. "HI"

Chapter 5:ADVANTAGES

Security: The RSA technique is frequently used for safe data transfer as it is thought to be extremely secure.

Public-key cryptography: The RSA algorithm needs two distinct keys for encryption and decryption since it is a public□key cryptography technique.

The data is encrypted using the public key and decrypted using the private key.

Key exchange: Secure key exchange, or the exchange of a secret key between two parties without transferring the key across a network, is possible with the use of the RSA algorithm.

Digital signatures: Digital signatures utilising the RSA technique allow a sender to sign a communication with their private key and a recipient to confirm the signature with the sender's public key.

Speed: Due to its effectiveness and speed, the RSA approach is well-suited for use in real-time applications.

Widely used: The RSA algorithm has been widely developed in a number of disciplines and applications, including online banking, e-commerce, and secure communications

CONCLUSION

The importance of encryption to India's technology infrastructure will only increase as it moves closer to becoming a digital superpower. India's transition from a developing to a developed country would be made easier if its foundation is established, and any democracy's foundation is elections. This will assist in preparing both India and the globe for the future.

Finally, cryptography is a fundamental component of digital security that cannot be overlooked. Its importance goes beyond simple encryption; it preserves the basis of confidence by guaranteeing the privacy and accuracy of the data that contemporary societies depend on. Cryptography will always be important for protecting data, facilitating safe transactions, and maintaining privacy. This means that strong cryptographic solutions will always be required.

REFERENCES

[1] M. K. Lim, Y. Li, C. Wang, and M. Tseng, "A literature review of blockchain technology applications in supply chains: A comprehensive analysis of themes, methodologies and industries," *Computers & Industrial Engineering*, vol. 154, p. 107133, Apr. 2021, doi: 10.1016/j.cie.2021.107133.

[2] Y.-X. Kho, S.-H. Heng, and J.-J. Chin, "A review of cryptographic electronic voting," *Symmetry*, vol. 14, no. 5, p. 858, Apr. 2022, doi: 10.3390/sym14050858.

[3] J. Bethencourt, D. Boneh, and B. Waters, "Cryptographic methods for storing ballots on a voting machine.," *Network and Distributed System Security Symposium*, Jan. 2007, [Online]. Available: http://crypto.stanford.edu/~dabo/pubs/papers/votestore.pdf

[4] H. Mishra and P. Maheshwari, "Blockchain in Indian Public Distribution System: a conceptual framework to prevent leakage of the supplies and its enablers and disablers," *Journal of Global Operations and Strategic Sourcing*, vol. 14, no. 2, pp. 312–335, Jun. 2021, doi: 10.1108/jgoss-07-2020-0044.