B.M.S College of Engineering

(Autonomous College under VTU)

Bull Temple Road, Basavanagudi, Bangalore - 560019

A report on

SEMINAR BASED ON SUMMER/WINTER INTERNSHIP

APPLICATIONS OF CRYPTOGRAPHY

Submitted in partial fulfillment of the requirements for the award of degree

BACHELOR OF ENGINEERING

IN

INFORMATION SCIENCE AND ENGINEERING

By

Samartha S (1BM19IS219)

Under the guidance of

S Preetha

Assistant Professor

DEPARTMENT OF INFORMATION SCIENCE & ENGINEERING

2021-22

BMS COLLEGE OF ENGINEERING

(Autonomous College under VTU)
Bull Temple Road, Basavanagudi, Bangalore – 560019

C E R T I F I C A T E

Certified that the Technical Seminar has been successfully presented at **B.M.S. College Of Engineering** by **Samartha S** bearing USN: **1BM19IS219** in partial fulfillment of the requirements for the VI Semester degree in **Bachelor of Engineering in Information Science & Engineering** of **Visvesvaraya Technological University, Belgaum** as a part of for the course - **Seminar Based on Summer/Winter Internship** Course Code – **20IS6SRITR** during academic year 2021-2022

Faculty Name: S Preetha

Designation: Assistant Professor

Signature:

Table of Contents

Sl. No.	Topic	Page No.
1	Abstract	4
2	Relevance of Cryptography	5
3	Domain Knowledge	6
4	Applications of domain	8
5	Pros and Cons of Cryptography	13
6	Conclusion	14
8	References	15

ABSTRACT

Over the past few decades, with the development of the World Wide Web and social media platforms, the internet has reached a level that merges with our lives, growing exponentially. The amount of data generated on the internet everyday is massive and the amount of information available on the internet increases exponentially everyday. As more and more users use the internet, more and more data is generated and this attracts more and more cyber criminals. Data security has become the main concern of anyone who uses the web. Data security ensures that our data is only accessible by the intended receiver and prevents any modification or alteration of data. In order to achieve this level of security, cryptography has played a major role. Various algorithms and methods have been developed to secure data. This report focuses on the various applications cryptography has in other major fields such as Machine Learning, Network Security, Blockchain and Cloud Computing.

RELEVANCE OF CRYPTOGRAPHY

Cryptography is associated with the process of converting ordinary plain text into unintelligible text and vice-versa. Cryptography is the process of hiding or coding information so that only the person a message was intended for can read it. The art of cryptography has been used to code messages for thousands of years and continues to have many applications in bank cards, computer passwords, and ecommerce.

Web applications have several endpoints, clients, dependencies, networks, and servers. To make these applications work, the physical systems need to make multiple requests across multiple networks that are often unprotected and open. Communications that take place in open and public networks are often the targets of attackers. In data and telecommunications, cryptography is necessary when communicating over any untrusted medium, which includes just about any network, especially the internet.

There are some specific security requirements that must be met:

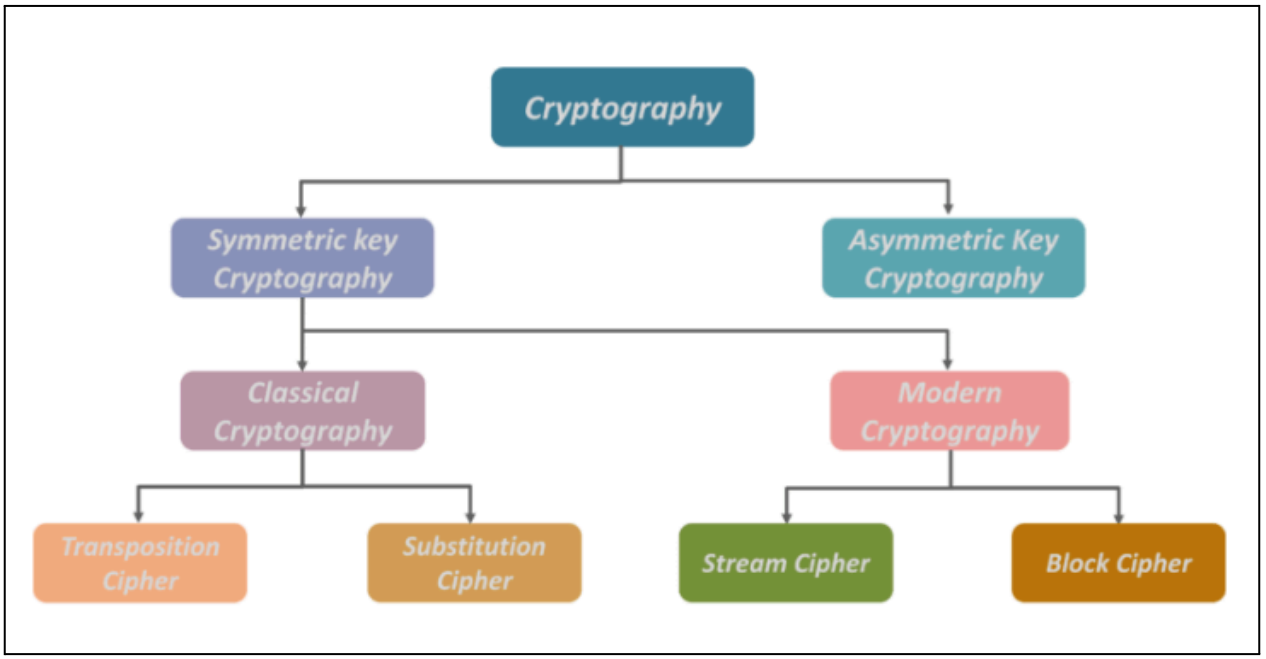
- **Authentication:** The process of proving one's identity
- **Confidentiality**: Ensuring that no 3rd party can read the message
- **Integrity:** Ensuring that the message received by the recipient has not been altered in any way

Cryptography is based on the above 3 principles. Hence cryptography not only protects the data on the internet from theft, but also ensures that it is not modified and also ensures user authentication.

Today most of us communicate via the internet, leaving valuable data everywhere unprotected. Information security should be the top priority for all application owners and users all around the world. Encryption and decryption algorithms of the highest security order should be implemented across all communication scenarios so that the sender and receiver can enjoy worry-free transactions. Thus cryptography is an extremely important field in today's world.

DOMAIN KNOWLEDGE

Cryptography is the practice and study of techniques for securing communication and data in the presence of adversaries. It is broadly concerned with algorithms and protocols that ensure the secrecy and integrity of data. It deals with developing and analyzing protocols which prevent malicious 3rd parties from accessing information shared between 2 entities. With historical roots, cryptography can be considered an old technique that is still being developed. Examples reach back to 2000 B.C., when the ancient Egyptians used “secret” hieroglyphics, as well as other evidence in the form of secret writings in ancient Greece or the famous Caesar cipher of ancient Rome.



Cryptography is broadly classified into two categories: Symmetric key Cryptography and Asymmetric key Cryptography. Symmetric key cryptography is an encryption system in which the sender and receiver of a message share a single, common key that is used to encrypt and decrypt the message. Asymmetric key cryptography is the encryption process where different keys are used for encrypting and decrypting the information. Now Symmetric key Cryptography is further categorized as Classical Cryptography and Modern Cryptography. Classical Cryptography is divided into Transposition Cipher and Substitution Cipher. On the other hand, Modern Cryptography is divided into Stream Cipher and Block Cipher.

Some important terminology:

- **Plain Text:** The original user-understandable message
- **Cypher Text:** The transformed message, as a result of encryption
- **Encryption:** The process of applying mathematical functions to PT to convert it to CT
- **Decryption:** The reverse process of encryption, converting CT to PT.
- **Key:** The encryption/decryption process requires a cryptographic key that tells the algorithm how to transform the plaintext into ciphertext.

Types of attacks:

- **Passive attacks:**
    - The attacker observes the messages, copies them and may use them for malicious purposes.
    - It is a danger to data confidentiality.
- **Active attacks:**
    - The attacker tries to modify or change the content of the messages.
    - It is a danger to Integrity and Availability of data.

Types of encryption:

- **Symmetric key encryption:**
    - The message is encrypted by using a key and the same key is used to decrypt the message.
    - This makes it easy to use but less secure.
    - It also requires a safe method to transfer the key from one party to another.
- **Asymmetric key encryption:**
    - There are 2 keys - public key and private key.
    - It uses two different keys to encrypt and decrypt the message.
    - It is more secure than the symmetric key encryption technique but is much slower.

APPLICATIONS OF THE DOMAIN

1. Cryptography and Network Security:

Organizations all over the world produce a lot of data every day thanks to the development of the World Wide Web, e-commerce applications, and social networks. Data security is the utmost critical issue in ensuring safe transmission of information through the internet. As more and more users connect to the internet, it attracts more and more cyber-criminals. The task of network security not only requires ensuring the security of end systems but of the entire network. A network security system typically relies on layers of protection and consists of multiple components including networking monitoring and security software in addition to hardware and appliances. All components work together to increase the overall security of the computer network.

Cryptographic techniques used in Network Security:

- **3DES:**

  Triple Data Encryption Standard, is a block cipher. 3DES is similar to DES (Data Encryption Standard), a method that uses 56-bit keys. Triple Data Encryption Standard is unique in that it uses symmetric-key encryption, using three distinct 56-bit keys. This method encrypts data a full three times, essentially transforming your singular 56-bit key into a 168-bit key.

- **Twofish:**

  Essentially, it is also a symmetric block cipher, with a block size ranging from 128 to 256 bits. The method works best for smaller CPUs as well as low-level hardware.

- **Advanced Encryption Standard (AES):**

  It is a symmetric encryption algorithm. The method makes use of a block cipher which fixes data at the rate of one at a time, with fixed size blocks.

- **RSA (Rivest, Shamir, Adelman):**

  The RSA algorithm utilizes public-key cryptography to transmit data through an unsafe network. It is an asymmetric cryptography algorithm, meaning that it functions on two distinct keys - the private key and public key.

2. Cryptography and Machine Learning:

Neural networks can protect their private information from other neural networks by discovering unique structures of encryption and decryption, without being taught a specific algorithm. Neural networks are generally not meant to be great at cryptography. The simplest neural networks cannot even compute XOR, which is basic to many cryptographic algorithms. But they can learn forms of encryption and decryption and protect the confidentiality of their data. Apart from learning "how" to encrypt, they can even learn "what" to encrypt.

Adversarially robust neural cryptography deals with the training of a neural-based model using an adversary to leverage the learning process in favor of reliability and trustworthiness. The adversary can be a neural network or a strategy guided by a neural network. These mechanisms are proving successful in finding secure means of data protection. Similarly, machine learning benefits significantly from the cryptography area by protecting models from being accessible to malicious users.

The neural networks Sender and Receiver must discover their own encryption techniques to keep their communication private and protected without the Intruder neural network understanding anything about it. Sender and Receiver neural networks periodically enhance themselves by optimizing their own models to beat the best version of Intruder neural network.

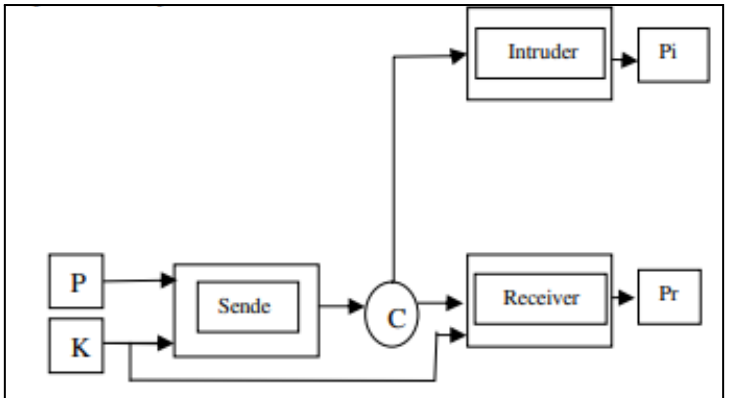


Figure. 1: Block diagram showing communication between Sender, Receiver and Intruder.

In the paper, they have proposed a "mix & transform" architecture. It has a first fully-connected (FC) layer, where the number of outputs is equal to the number of inputs. The plaintext and key bits are fed into this FC layer. The FC layer is followed by a sequence of convolutional layers.

These convolutional layers learn to apply some function to groups of the bits mixed by the previous layer, without an a priori specification of what that function should be.

The result obtained:

Iteration	Receiver's Reconstruction Error	Intruder's Reconstruction Error
0	7.98	7.99
200	7.91	7.52
400	7.88	7.56
800	5.33	6.11
1000	2.45	6.07
2000	0.83	6.76
4000	0.08	7.26
8000	0.02	7.46
10000	0.01	7.51
15000	0.01	7.58
20000	0.01	7.50

3. Cryptography and Blockchain:

Blockchain is a peer-to-peer network; the word 'blockchain' is made up of two separate terms, 'block' and 'chain'. A block being referred to a collection of data, alias data records, and chain being referred to a public database of these blocks, stored as a list. These lists are linked using cryptography, making it the most essential and fundamental requirement for creating a blockchain. In blockchain, digital encryption technology has a core position. The security of user information and transaction data is a necessary condition for the promotion of blockchain. Due to its distributed nature, blockchain stores all user transaction information on the blockchain, which has high requirements for the security. Blockchain is a decentralized peer-to-peer network. Nodes do not need to trust each other and there is no central node. Therefore, transactions on the blockchain also need to ensure the security of transaction information on unsecured channels.

Blockchains make use of two types of cryptographic algorithms, asymmetric-key algorithms, and hash functions. Hash functions are used to provide the functionality of a single view of blockchain to every participant. Blockchains generally use the SHA-256 hashing algorithm as

their hash function.

Cryptographic hash functions provide the following benefits to the blockchain:

- **Avalanche effect** - A slight change in the data can result in a significantly different output.
- **Uniqueness** - Every input has a unique output.
- **Deterministic** - Any input will always have the same output if passed through the hash function.
- **Quickness** - The output can be generated in a very small amount of time.
- **Reverse engineering is not possibl**e, i.e. we cannot generate the input by having the output and the hash function.

One of the major parts of asymmetric-key cryptography is digital signatures. Digital signatures provide integrity to the process; they are easily verifiable and cannot be corrupted. They also hold the quality of non-repudiation, making them similar to the signatures in the real-world. The digital signatures ensure that the blockchain is valid and the data is verified and correct. Hashing, public-private key pairs, and the digital signatures together constitute the foundation for the blockchain. These cryptographic features make it possible for blocks to get securely linked by other blocks, and also ensure the reliability and immutability of the data stored on the blockchain.

4. Cryptography and Cloud Computing

Cloud computing allows an organization to use IT services delivered via the internet instead of maintaining your own physical servers. Cloud Computing refers to controlling, arranging, and getting to the equipment and programming assets remotely. It offers online data storage, infrastructure, and applications. Cloud Computing gives customers a virtual computing environment on which they can store information and run applications. But, Cloud computing has presented security challenges since cloud administrators store and handle customer information. Cloud computing services are subject to cyber-attacks and data breaches.

Cryptography in the cloud employs encryption techniques to secure data that will be used or stored in the cloud. It allows users to conveniently and securely access shared cloud services, as any data that is hosted by cloud providers is protected with encryption. Cryptography in the cloud protects sensitive data without delaying information exchange.

There are various approaches to extending cryptography to cloud data. Many companies choose to encrypt data prior to uploading it to the cloud altogether. This approach is beneficial because data is encrypted before it leaves the company's environment, and data can only be decrypted by authorized parties that have access to the appropriate decryption keys. Other cloud services are capable of encrypting data upon receipt, ensuring that any data they are storing or transmitting is protected by encryption by default.

There are two primary types of cloud cryptography:

A) Data-in-transit: When data is moving between end points.
B) Data-at-rest: sensitive data that is stored in corporate IT structures such as servers, disks, or cloud storage services.

The 2 most popularly used cryptographic algorithms in cloud cryptography are: DES (Data Encryption Standard) and RSA (Rivest-Shamir-Adleman). Simulation result showed that DES has better performance than RSA. It showed that the throughput of the DES algorithm is much better than the throughput of the RSA algorithm. The results showed that DES is better than all other algorithms in throughput and power consumption. The main drawbacks of DES Algorithms are that it can suffer from key distribution and key agreement problems, But RSA consumes large amounts of time to perform encryption and decryption operations.

PROS AND CONS OF CRYPTOGRAPHY

Pros:

- **Ensures Confidentiality** - Encryption technique can guard the information and communication from unauthorized revelation and access of information.
- **Provides Authentication** - The cryptographic techniques such as MAC and digital signatures can protect information against spoofing and forgeries.
- **Ensures Data Integrity** - The cryptographic hash functions are playing a vital role in assuring the users about the data integrity.
- **Non-repudiation of data** - The digital signature provides the non-repudiation service to guard against the dispute that may arise due to denial of passing message by the sender

Cons:

- A strongly encrypted, authentic, and digitally signed information can be difficult to access even for a legitimate user at a crucial time of decision-making.
- High availability, one of the fundamental aspects of information security, cannot be ensured through the use of cryptography. Other methods are needed to guard against the threats such as denial of service or complete breakdown of the information system.
- Another fundamental need of information security of selective access control also cannot be realized through the use of cryptography. Administrative controls and procedures are required to be exercised for the same.
- Cryptography does not guard against the vulnerabilities and threats that emerge from the poor design of systems, protocols, and procedures.

CONCLUSION

As we have seen, cryptography is a very important field that has very important applications in several other fields. We have covered its applications in just a few fields, but there are a lot of other fields such as e-commerce, autonomous vehicles, defense organizations etc. in which cryptography has a huge application. As technology advances, the importance of cryptography will also increase and more and more data will be generated and protecting and safeguarding the huge amount of data will be very important.

PAPERS REFERRED

1. *A review paper on Cryptography* by Abdalbasit Mohammed Qadir and Nurhayat Varol (2019)
2. *Research on Various Cryptography Techniques* by Yahia Alemami, Mohamad Afendee Mohamed, Saleh Atiewi (2019)
3. *Bridging machine learning and cryptography in defense against adversarial attacks* by Olga Taran, Shideh Rezaeifar, and Slava Voloshynovskiy (2018)
4. *Application of Machine Learning in Cryptography* by Vikrant Shende and Meghana Kulkarni (2020)
5. *Review on Network Security and Cryptography* by Shyam Nandan Kumar (2017)
6. *Cloud Security: A Security Aspect* by Felix Bentil and Isaac Lartey (2021)
7. *Research on the Application of Cryptography on the Blockchain* by Zhai, Yang, Li, Qiu and Zhao (2019)
8. *A Review Paper On Concepts Of Cryptography And Cryptographic Hash Function* by Dr. RK Gupta (2020)
9. *Analysis of Cryptography Encryption for Network Security* by Jyothi, Dr. Prasad and Dr. Mojjada (2020)
10. *SoK of Used Cryptography in Blockchain* by Raikwar, Gligoroski and Kralevska (2019)
11. *A Study of Blockchain-Based Cryptosystems* by Thyagarajamurthy and Anusha M (2021)
12. *Use of cryptography in Cloud Computing* by Jaber and Zolkipli (2017)
13. *A Simple and Secured Cryptography System of Cloud Computing* by Islam, Chaudhury and Islam (2019)
14. *A study on Role and Applications of Cryptography Techniques in Cloud Computing (Cloud Cryptography)* by Waseem Akram (2019)
15. *A study on Blockchain and Cryptography* by Banger, Mittal, Khowal and Mehta (2020)