A Review Paper on Cryptography & Network Security

Anush Sharma

(Assistant Professor, Dept. of Computer Science and Engineering) HIET Group of Institutions, Shahpur

Rishav Kumar

(Department of Computer Science and Engineering) HIET Group of Institutions, Shahpur

Abhishek Choudhary

(Department of Computer Science and Engineering) HIET Group of Institutions, Shahpur

Abhinash Sandhu

(Department of Computer Science and Engineering) HIET Group of Institutions, Shahpur

ABSTRACT

In today's digital age, the need for secure communication and data protection is paramount. Cryptography plays a vital role in achieving these goals by employing various encryption algorithms. This review paper aims to explore the different encryption techniques used in cryptography, their strengths, weaknesses, and real-world applications. We delve into symmetric and asymmetric encryption, hash functions, and key management. Additionally, we discuss the challenges faced in implementing secure cryptographic systems, such as key distribution and algorithm vulnerabilities. Furthermore, we explore the advancements in cryptography and the future directions it may take. By understanding the intricacies of cryptography, we can better safeguard our sensitive information and ensure the integrity and confidentiality of data in the digital environment.

INTRODUCTION:

Cryptography is a fascinating field that focuses on securing information and communication in the digital world. It involves the use of mathematical algorithms and ways to convert data into a secret code, making it unreadable to unauthorized persons.

By using encryption and decryption processes, cryptography ensures the confidentiality, integrity, and authenticity of data. It plays a crucial role in guarding sensitive information like passwords, financial

transactions, and private messages.

It(cryptography) encompasses ways and algorithms that transfigure textbook into an translated law, which we relate to as cipher textbook. This law can only be decrypted by individualities enjoying the key or word. It's like the retired secrets of communication.

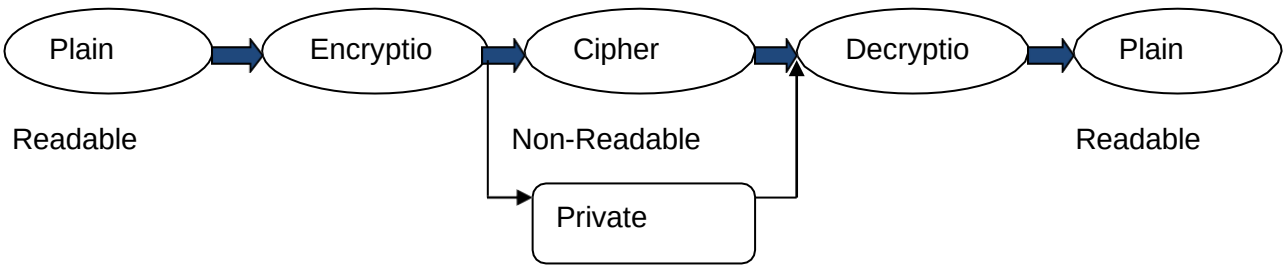
The rapid-fire advancement of Internet technology and information technology has led to an increase, in the number of individualities connecting to the Internet. Unfortunately this has also redounded in a rise in druggies who essay to attack and disrupt the network by employing styles similar, as websites, deceptive emails Trojan nags and backdoor contagions. As a result the fast development of the ultramodern Internet technology and information technology caused every illegal stoner to attack and destroy the network by using the fake websites, fake correspondence, Trojan steed and backdoor contagion at the same time.

TYPES OF CRYPTOGRAPHY:

- Symmetric Cryptography
- Asymmetric Cryptography
- Hash Cryptography

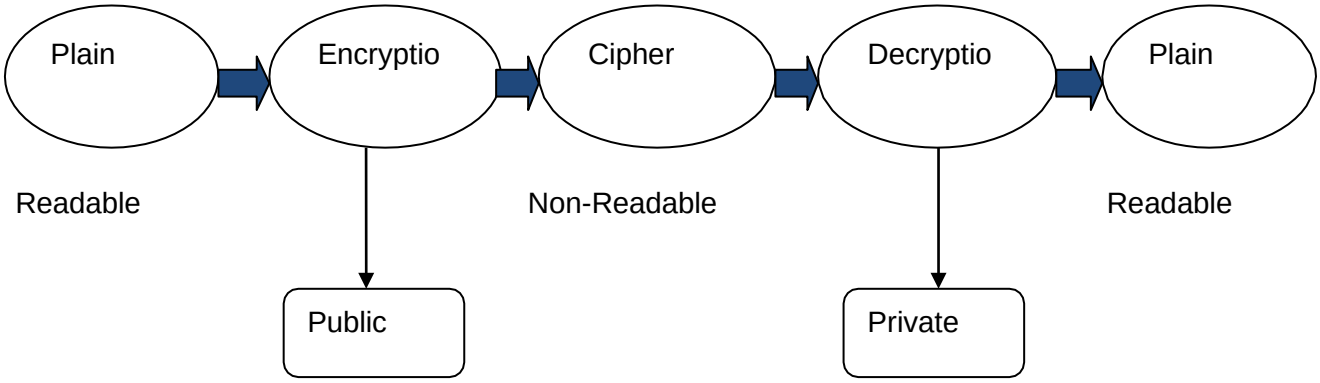
Symmetric Cryptography:

Symmetric crucial cryptography refers to an encryption system in which both the sender and receiver use a participated key, to cipher and decipher dispatches. These systems are known for their speed and simplicity. still a challenge lies in swapping the key, between the sender and receiver. Common exemplifications of cryptography systems include Data Encryption Standard(DES) and Advanced Encryption Standard(AES).



Asymmetric Cryptography:

In asymmetric crucial cryptography, we use a brace of keys a public key and a private key. The public key is used for cracking information, while the private key is used for decoding it. Indeed if the public key is known to everyone, they can not crack the communication because only the person with the private key can do that. It's like having a special secret that only they can understand. So, indeed if others have the public key, they can not unleash the communication without the private key.



Hash Cryptography:

In this algorithm, rather of using a key, a fixed length hash value is calculated grounded on the textbook. This hash value is like a unique point of the textbook and ensures that the factual contents of the textbook can not be recaptured. Operating systems frequently use hash functions to encrypt watchwords, making them more secure. It's like creating a secret law that can not be reversed to reveal the original information. So, indeed if someone gets hold of the hash value, they can not figure out the original textbook from it. It's a clever way to cover sensitive information like watchwords.

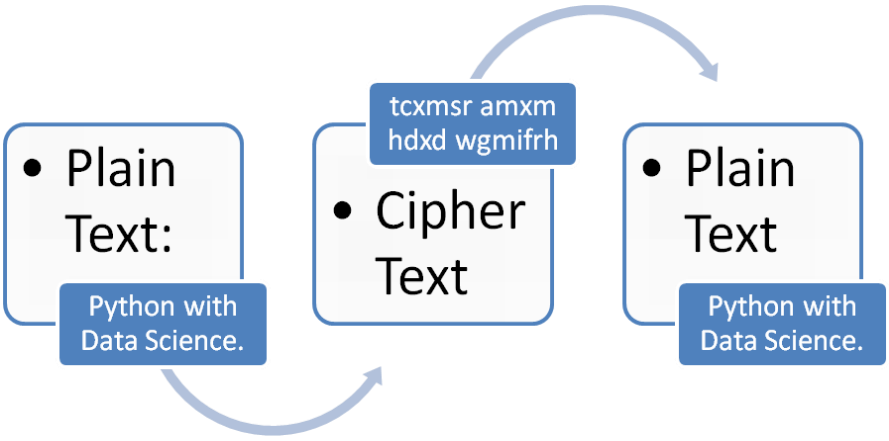
CRYPTOGRAPHY PROCESS:

- **Plain Text:** It refers to the dispatches that need to be decoded or translated. It's like taking regular words and turning them into secret canons**.**
- **Encryption:** It means taking information and turning it into secret law. This process of turning regular textbook into cipher content is called encryption. It's like using a secret language to keep the information safe and secure.
- **Cipher Text:** When we relate to" reckon content," we are talking about the decoded communication. It's

like taking regular textbook and transubstantiating it into a secret law that isn't fluently readable. So, the decoded communication is called cipher content. It's a way of keeping information hidden and defended.

- **Decryption:** When we talk about decryption, it means taking the decoded or cipher content and transubstantiating it back into the original, readable form, which we call plain content..

Decryption



Encryption

SECURITY MECHANISM:

- **Confidentiality:** Confidentiality means that only the people who are supposed to see the information can see it. It's like having a secret code that only the right people can understand.

- **Integrity:** Integrity means that the digital information is protected from any unwanted changes or tampering. It ensures that only the authorized people can access or make changes to the information. So, it's like having a lock on the information to keep it safe from any unauthorized modifications.

- **Authentication:** Authentication is like proving who you are to a security system. It's like showing your ID card or entering your username and password to confirm your identity when you want to access a website. It's a way to make sure that only the right people can get in.

- **Non-Repudiation:** Non-repudiation means that if someone signs a document or data with their signature key, they can't later deny that they signed it. It's like having a receipt for something you bought - you

can't say you didn't buy it when there's proof that you did.

- **Access Control:** Access control is like a security system that checks who you are before letting you in. It can ask for things like usernames, passwords, fingerprints, or special cards to make sure you're the right person. It's like having a secret code or key to unlock a door and only the right people have it.

- **Availablity:** Availability means that everything you need, like systems, apps, and data, is always there when you want to use it. It's like having your favorite app on your phone, ready to use whenever you need it. You don't have to wait or worry about it not being available.

FUTURE SCOPE:

- **Quantum-Resistant Cryptography:** With the development of important amount computers, traditional styles of keeping data secure may come vulnerable. So, experimenters are working on amount- resistant cryptography to make sure our data stays safe indeed in a world with amount computers.
- **Blockchain and Cryptocurrencies:** Cryptocurrencies like Bitcoin calculate on cryptography to keep deals and holdalls secure. The future of cryptocurrencies and blockchain technology depends on perfecting cryptographic ways to make them indeed more secure, private, and scalable.

- **IoT (Internet of Things) Security**: As further and further bias come connected to the internet, it's important to keep the communication between these bias and networks secure. Cryptography plays a big part in making sure the data transmitted by these bias remains nonpublic and can not be tampered with..

- **Homomorphic Encryption**: This fancy term refers to a type of encryption that allows calculations to be done on translated data without demanding to decipher it first. It's like doing calculation with secret figures, which can be useful for secure data processing in the pall while keeping everything private and secure.

- **Post-Quantum Cryptography:** As quantum computers become more powerful, the encryption methods we currently use might not be enough to keep our data safe. So, researchers are working on developing new encryption algorithms and protocols that can withstand attacks from quantum computers.

- **Secure Communication Protocols**: When we send data over the internet, it's important to make sure it stays secure during transmission. That's where secure communication protocols like TLS and **HTTPS** come in. They help protect our data from threats while it's in transit.

CONCLUSION:

In simpler terms, cryptography is all about keeping our data safe and secure. It's like putting a lock on a box to make sure no one can open it without the right key. Cryptography uses special techniques to scramble our data so that only authorized people can access it. It's important because it helps protect our personal information, like passwords and credit card numbers, when we send them over the internet. As technology advances, cryptography is constantly evolving to stay one step ahead of hackers and keep our information safe.

REFERENCES:

[1] **Mr.Janani Ramesh**, February 8, 2022 https://easychair.org/publications/preprint/DD5v

[2] **Waliyullahi O. Zakariyah**, 08 December2021.
https://www.researchgate.net/publication/356879084_Cryptography

[3] Ajay Ohri *What is cryptography*, date published: Feb 2, 2021

https://www.google.com/amp/s/www.jigsawacademy.com/blogs/cybersecurity/what-is-cryptography

[4] Jayanthi Manikandan *Basics of cryptography* date published: April 2018

https://resources.infosecinstitute.com/topic/basics-of-cryptography- thepractical

[5] R. E. Frazier, 2004, *data encryption techniques*,

http://catalog.com/sft/encrypt

[6] Gary C. Kessler, 1998, an overview of cryptography, http://www.garykessler.net/library/crypto

[7]* Jennifer Tauser, 2005, *Encryption is the most important tool for Internet security and privacy