Study of Cryptography In Cyber Security

Rutuja Anant Velnaskar[1], Sayali Bharat Mahadik[2], Prof. Sadanand Sachchidanand Dongare[3]
[1, 2] Dept of Computer Science
[3]Asst. Professor, Dept of Computer Science
[1, 2, 3] DUBSS College, Dapoli,

Abstract- *Cryptography is a process that secures information and communication in the form of secret code. In this, data or a message is encrypted into ciphertext from hacking. Using encryption and decryption keys, we can lock and unlock the data or message. Key mechanism is very important in cryptography. It includes many algorithms against leaking data while transferring from one user to another. This algorithm consists of encryption and decryption also. To make a secure connection between sender and receiver to communicate with privacy, cryptographic protocols are used. It also has many challenges of cryptography. While transferring data, third parties make many attacks on finding actual data. Hence, security mechanisms in cryptography are very strict and strong. In this, there are some benefits and drawbacks of cryptography, and it also has legal issues with it. Applications of cryptography are useful nowadays because scams and spam are increased.*

I. INTRODUCTION

Cryptography is a technique which is used for secure information and communication in the form of code. Each character in plain text is substituted by another character forming the text called cipher text. It uses encryption algorithm and decryption algorithm for securing data. Encryption means converting plain text into cipher text, means readable data into unreadable data. Decryption means converting cipher text back to the plain text. It is used for protect personal information from third party. The sender encrypts its message using key and similar to receiver decrypt sender's message using either same key or different key. The encrypted message is readable for third party but not understandable because, it is in cipher text. Cryptography consists of some mathematical concept and rule base calculation called Algorithm for secure information and communication. There are some Algorithms behind encryption of data.In today's life Cryptography is crucial for several reasons: for secure online transaction and private communication. Cryptography is important for protecting sensitive information such as credit card numbers and personal data during online transaction. Cryptography ensures confidential communication over the internet protecting email messages and phone calls and protects data.

II. HISTORY

The origins of cryptography are found by Roman and Egyptian societies. They used early forms of secret writing to protect their messages. Hieroglyphs Cryptography, Caesar Cipher, Vigenere Cipher, Hebern rotating machine, Enigma machine are some ancient types of Cryptography. The word cryptography comes from Greek word 'kryptos' means 'hidden' and 'graphy' means to 'writing' these 'hidden writing' has been advancing for thousands of years in 1500 BC a Mesopotamian scribe used cryptography to conceal a formula for pottery glaze. This example is first known use of cryptography to hide secret information.

III. TYPES OF CRYPTOGRAPHY

Cryptography has three types:

1. Symmetric key Cryptography
2. Asymmetric key cryptography
3. Hash Function

1) Symmetric key Cryptography:

Symmetric key cryptography it is also known as private key cryptography .In this type of cryptography encryption and decryption key are same .The sender and receiver can use this same key for encrypt or decrypt message. Example of symmetric key cryptography is blowfish. DES,AES are symmetric key algorithm.

2) Asymmetric key cryptography:

Asymmetric key cryptography is also known as public key Cryptography. In this type of cryptography, encryption and decryption keys are different. The sender and receiver can use different key for encryption and decryption. For eg., Sender is used public key for encrypt the plane text into cipher text and receiver is used private key for decrypt the cipher text into plane text. It consists RSA Algorithm.

3.) Hash function:

A hash function has mathematical formula that takes input data of any size and produces fixed size of output. It is called as hash value or digest. Data integrity, password storage, digital signature, data de-duplication are the hash function's uses in cryptography. It consists of SHA-256 Algorithm,MD-5 Algorithm.

IV. CRYPTOGRAPHIC PROTOCOLS

1. PGP - pretty good privacy:

It is open source freely available software package. PGP protocol is used for securely transforming electronic mail from one user to another. PGP is safe, if all employees or user used PGP correctly or securely. PGP is one of the most secure method to protect our data. PGP is now on an internet standards track(RFC 3156). Using digital signature it provides authentication. The function of PGP services are digital signature, message encryption, compression, email-compatibility.

2. SSL - Secure Socket Layer:

Netscape developed SSL in 1994. It's version 2 and 3 where release in 1995 .SSL is design to provide security and compression services to data generated from the application layer the data receive from the application is compressed signed and encrypted. Essel provide several services on data received from the application layer such as fragmentation, compression, message integrity, confidentiality and framing.

V. CHALLENGES OF CRYPTOGRAPHY

1) Key Management: As more users gain access to a key, key management may become more complicated. Cryptographic keys must be generated, distributed, and stored securely. The system as a whole may be at risk due to compromised keys.

2) **Performance:** Cryptographic operations can be computationally demanding, which might affect performance, particularly for devices with limited resources. Delays may result, and the user experience may suffer. Enhance performance for devices with limited resources.

3) **Algorithm Security:** Cryptographic algorithms need to be resistant to a range of threats. Existing algorithms are at risk from growing computing capability, particularly quantum computing.

4) **Side-Channel Attack:** These attacks take advantage of data obtained from a cryptographic system's actual physical implementation.

5) **Interoperability:** Compatibility problems may arise because different systems and applications employ different encryption standards. One of the biggest challenges is ensuring interoperability while preserving security.

6) **User Errors:** Cryptographic security can be compromised by human error, such as using weak passwords or disregarding security procedures. Security features of cryptographic algorithms are used to guard against human error.

VI. SECURITY MECHANISM IN CRYPTOGRAPHY

1) Encipherment: The plain text is converted to cipher text after encryption. Your data gets transformed into a cipher text since you don't want anyone to view it. This is produced by cryptography algorithms and results in a mathematical language. The encryption algorithm is dependent on the confidentiality of your data.

2) Digital Signature: By making digital data visible to the public, this security measure is accomplished. An audience electronically verifies this type of electronic signature. Digital signatures are extremely secure and are done in a very covert manner.

3) Data Integrity: A brief check value generated by a particular procedure from the data itself is appended to the data by the mechanism. The receiver uses the receiver data to generate a new check value, which is then compared to the original check value. The integrity of the data has been maintained if both values are the same.

4) Authentication Exchange: The security technique that deals with identification to be known in communication is called authentication exchange. This is accomplished at the TCP/IP layer by using a two-way handshaking method to verify whether or not data is transmitted. In order to establish their identities, two entities share the identical message.

VII. BENEFITS OF CRYPTOGRAPHY

1) Confidentiality: If you don't want to show your data to anyone, we can secure that data using cryptography. This ensures that only the intended recipient can read the data. To achieve confidentiality, an encryption key is used. Cryptography is the study of mathematics that allows private messages to be securely transmitted over any unsecure channel.

2) Authentication: Authentication mechanism helps establish proof of identities. Cryptography facilitates authentication and verification mechanism allowing users to prove their identity. Authentication helps protect your data. Authentication helps protect your data from breaches and reduces the risk of cybercrime. Authentication tells us with confidence that our digital signal signature is true.

3) Data integrity: It helps in verifying that information has not been altered or tampered with during transmission. Data integrity helps keep your data safe. Data integrity supports accurate data inside and decision.

4) Non-repudiation: In the legal field, the digital signature is considered handwritten. Non-repudiation helps to verify the identity of the sender and the authenticity of the data.

VIII. LEGAL ISSUES WITH CRYPTOGRAPHY

Cryptography has historically been used for military information collection, and its use by terrorists and criminals could make it more difficult for law enforcement to execute the law. Therefore, it is not surprising that governments often impose restrictions on its use. The intricate mathematical nature of the associated algorithms gives rise to additional legal concerns that are related to patents.The legal issues with cryptography are divided into three categories**:**

1)Export Control Issues
2)Import Control Issues
3)Patent-Related Issues

IX. APPLICATION OF CRYPTOGRAPHY

1) Secure Communications: Cryptography is used to secure calls, messages, emails etc. Cryptography is the most secure way to communicate between a client, program, and server. The most common use of cryptography is to encrypt communications within a system securely. When the Internet was developed, its use was decreasing, but now the Internet is used in every field, such as education, government work, and banking etc. example of web browser and web server or email client and email server.

2) End-to-End Encryption: Encryption is not widely used in email. Email is encrypted when it travels from server to server and from server to you. You can read data on the mail server and on your system. Email is a good example of end-to-end encryption. Truly secure messaging systems are only the sender and receiver can read the messages; those were encryption has been built in from the start. WhatsApp is good example of end-to-end Encryption. If you want to hide your private chat in WhatsApp, end-to-end encryption is used for that.

3) Storing Data: We store whatever important data you have and that Data is very important to those who created it. We use encryption to hide our system passwords. If you don't want anyone to see your important contact numbers, including private ones, you encrypt them. So your hidden data remains secure. No one can read it.

4) Storing Password: The main function of storing passwords is to store passwords. The password you save is stored using a hashing algorithm. The advantage of storing your password in a hash in your system is that it remains secret and cannot be seen by anyone. If your data is leaked, attackers only see the password in the hash. Hash algorithms do not harm us, so we can secure our system.

X. CRYPTANALYSIS

The science and art of cracking secret codes is known as cryptanalysis, just as cryptography is the science and art of constructing them. We must learn cryptanalysis techniques in addition to cryptography techniques. This is necessary to discover how weak our cryptosystem is, not to crack other people's codes. The study of cryptanalysis aids in the development of more effective secret codes. Four typical cryptanalysis attack types are as follows:

1) Cipher text-Only Attack:

Third parties can only access a portion of the cipher text in a cipher text-only assault. They look for the plaintext and the matching key. They are presumed to be aware of the algorithm and capable of intercepting the cipher text. Since they can only require the cipher text for this attack, the cipher text-only attack is the most likely. To prevent an opponent from decrypting a message, a cipher needs to be extremely resistant to this kind of assault.

2) Brute-Force Attack:

Using the exhaustive-key-search or brute-force approach, third parties attempt to make use of every key available. They are assumed to be familiar with the algorithm and the key domain, which is the list of all potential keys. They use every key. They can find the key to decrypt the cipher text using the intercepted cipher until the plaintext makes sense. In the past, utilizing a brute-force approach was challenging; today, using a computer makes it easier. There must be a huge number of potential keys in order to stop this kind of attack.

3) Statistical Attack:

Certain intrinsic properties of the plaintext language can be used by the cryptanalyst to initiate a statistical attack. For example, we are aware that the letter E is the one that appears in English texts the most. After identifying the most frequently used character in the ciphertext, the cryptanalyst deduces that the corresponding character in the plaintext is E. The analyst can locate the key and use it to decode the communication once they have identified a few pairs. The cipher should conceal the language's characteristics in order to thwart this kind of assault.

4) Pattern Attack:

Certain ciphers may conceal linguistic features while producing patterns in the ciphertext. It is crucial to select ciphers that make the ciphertext appear as random as possible because a cryptanalyst might employ a pattern attack to crack the cipher.

5) Chosen-plaintext Attack:

The selected plaintext assault is comparable to the known-plaintext attack; however, the attacker has selected the plaintext/ciphertext pairs herself. For example, if third parties had access to the sender's computer, this may occur. They have the ability to intercept the generated ciphertext and select some plaintext. Since the key is typically built in the program that the sender uses, they obviously do not have it. Although it is significantly less likely to occur, this kind of attack is much simpler to carry out.

6) Chosen-Cipher Text Attack:

With the exception of a cryptanalyst selecting some cipher text and decrypting it to create a cipher text/plaintext combination, the chosen-cipher text attack is comparable to the chosen-plaintext attack.

XI. CONCLUSION

Bringing it altogether, in this digital era, encryption is significant tool for safeguarding sensitive data. It is crucial for safe online communication and transactions and offers a powerful way to guarantee the integrity, secrecyand validity of data. Despite all the advantages, it also has a number of disadvantages, such as performance overhead, complexity problems with key management, and susceptibility to cyber-attacks. In spite of these difficulties, cryptography is still an essential part of contemporary cyber security, and its significance will only increase as the digital environment changes.

1. Put strong and secure cryptographic algorithms and protocols into place in order to optimize the advantages of cryptography.
2. To safeguard encryption keys, employ secure key management procedures.

REFERENCES

[1] History of Cryptography https://www.digicert.com/blog/the-history-of-cryptography#:~:text=In%201500%20BC%2C%20a%20Mesopotamian,almost%20every%20major%20early%20civilization
[2] Types of Cryptography https://www.shiksha.com/online-courses/articles/types-of-cryptography/
[3] Behrouz A. Forouzan and DebdeepMukhopadhyay“Cryptography and Network Security” 2nd Edition, McGraw Hill Education (India) Private Limited
[4] Security Mechanism in Cryptography https://www.geeksforgeeks.org/types-of-security-mechanism/
[5] Benefits of Cryptography https://www.tutorialspoint.com/cryptography/benefits_and_drawbacks.htm
[6] Legal Issues with Cryptography https://www.informit.com/articles/article.aspx?p=170967&seqNum=14