International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 01 | January - 2023 Impact Factor: 7.185 ISSN: 2582-3930

Research Paper on Cyber Security and Cryptosystem

Apurva Khangal[1], Ayush Sapariya[2]

[1]Department of Computer Engineering, K.J. Somaiya Polytechnic
[2]Department of Computer Engineering, K.J. Somaiya Polytechnic

---

Abstract – Cyber security refers to every aspect of protecting an organization and its employees and assets against cyber threats or attacks As cyber-attacks have become more common and sophisticated and corporate networks grow more complex, a variety of cyber security solutions are required to mitigate corporate cyber risk. Cryptosystem is one of the ways to prevent these cyber-attacks.

***Key Words*:** cyber-attacks, encryption algorithm, decryption algorithm, cipher system.

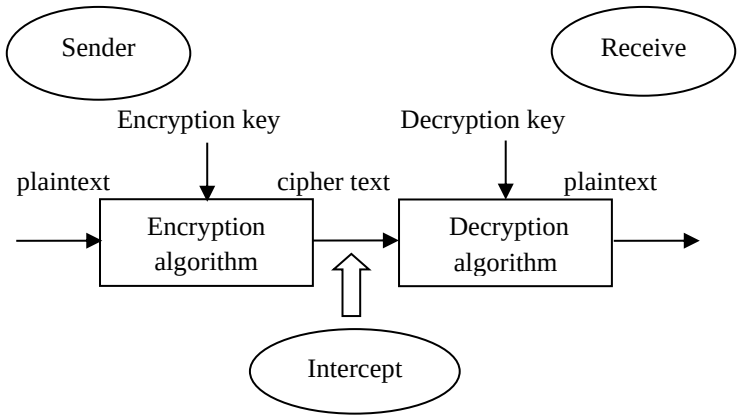
1. INTRODUCTION

Cryptosystem is a method of protecting information and communication through the use of codes, so that only for whom the information is intended can read and process it.

In computer science, cryptosystem refers to secure information and communication techniques derived from mathematical concepts and a set of rule-based calculations called algorithms, to transform messages in ways that are hard to decipher. These deterministic algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on the internet and confidential communications such as credit card transactions and email.

2. Components of Cryptosystem

- **Plaintext:** It is the data to be protected during transmission.
- **Encryption Algorithm:** It is a mathematical process that produces a cipher text for any given plaintext and encryption key. It is a cryptographic algorithm that takes plaintext and an encryption key as input and produces a cipher text.
- **Cipher text:** It is the scrambled version of the plaintext produced by the encryption algorithm using a specific the encryption key. The cipher text is not guarded. It flows on public channel. It can be intercepted or compromised by anyone who has access to the communication channel.
- **Decryption Algorithm:** It is a mathematical process, that produces a unique plaintext for any given cipher text and decryption key. It is a cryptographic algorithm that takes a cipher text and a decryption key as input, and outputs a plaintext. The decryption algorithm essentially reverses the encryption algorithm and is thus closely related to it.
- **Encryption Key:** It is a value that is known to the sender. The sender inputs the encryption key into the encryption algorithm along with the plaintext in order to compute the cipher text.
- **Decryption Key:** It is a value that is known to the receiver. The decryption key is related to the encryption key, but is not always identical to it. The receiver inputs the decryption key into the decryption algorithm along with the cipher text in order to compute the plaintext.
- The **illustration** shows a sender who wants to transfer some sensitive data to a receiver in such a way that any party intercepting or eavesdropping on the communication channel cannot extract the data. The objective of this simple cryptosystem is that at the end of the process, only the sender and the receiver will know the plaintext.



3. How it works?

Cryptosystem takes a plaintext (also known as a clear text) and turns it into something that can only be understood by the intended receivers. Anyone else who somehow gets their hands on this piece of information shouldn't be able to understand it.

The practice of turning a plaintext into a cipher text, encryption practices is followed. To turn a cipher text into a plaintext, decryption practices are followed.

For example-

The transformation can be represented by aligning two alphabets; the cipher alphabet is the plain alphabet rotated left or right by some number of positions. For instance, here is a Caesar cipher using a left rotation of three places, equivalent to a right shift of 23 (the shift parameter is used as the key):

Plain	A	B	C	D	E	F	G	H	I	J	K	L	M
Cipher	X	Y	Z	A	B	C	D	E	F	G	H	I	J

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
K	L	M	N	O	P	Q	R	S	T	U	V	W

When encrypting, a person looks up each letter of the message in the "plain" line and writes down the corresponding letter in the "cipher" line.
Plaintext:
THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG
Cipher text:
QEB NRFZH YOLTK CLU GRJMP LSBO QEB IXWV ALD

There are various techniques employed in order to encrypt a plaintext: Symmetric encryption, asymmetric encryption, hashing functions, block chain and digital signatures are some of the most prominent encryption techniques. They are often employed along with other cyber security measures.

4. Goals of Cyber security

1. **Confidentiality:** The degree of confidentiality determines the secrecy of the information. The principle specifies that only the sender and receiver will be able to access the information shared between them. Confidentiality compromises if an unauthorized person is able to access a message.
   For example, let us consider sender A wants to share some confidential information with receiver B and the information gets intercepted by the attacker C. Now the confidential information is in the hands of an intruder C.

2. **Authentication:** Authentication is the mechanism to identify the user or system or the entity. It ensures the identity of the person trying to access the information. The authentication is mostly secured by using username and password. The authorized person whose identity is preregistered can prove his/her identity and can access the sensitive information.

3. **Integrity:** Integrity gives the assurance that the information received is exact and accurate. If the content of the message is changed after the sender sends it but before reaching the intended receiver, then it is said that the integrity of the message is lost.

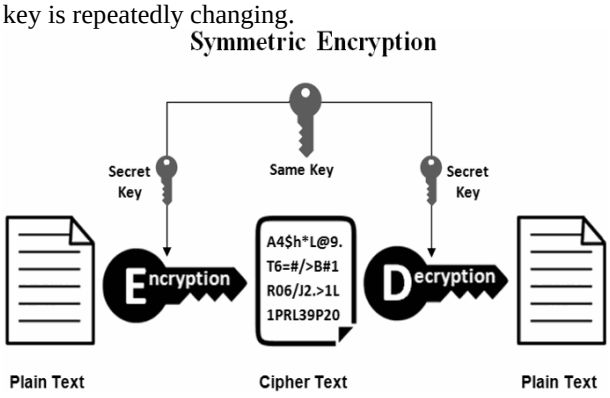
4. **Non-Repudiation:** Non-repudiation is a mechanism that prevents the denial of the message content sent through a network. In some cases the sender sends the message and later denies it. But the non-repudiation does not allow the sender to refuse the receiver.

5. **Access control:** The principle of access control is determined by role management and rule management. Role management determines who should access the data while rule management determines up to what extent one can access the data. The information displayed is dependent on the person who is accessing it.

6. **Availability:** The principle of availability states that the resources will be available to authorize party at all times. Information will not be useful if it is not available to be accessed. Systems should have sufficient availability of information to satisfy the user request.

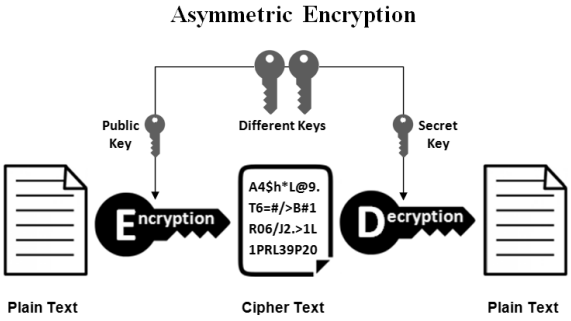
5. Techniques

- **Symmetric Key:** Symmetric key cryptosystem is a type of encryption scheme in which the similar key is used both to encrypt and decrypt messages. Such an approach of encoding data has been largely used in the previous decades to facilitate secret communication between governments and militaries. Symmetric-key cryptosystem is called a shared-key, secret-key, single-key, one-key and eventually private-key cryptosystem. With this form of cryptosystem, it is clear that the key should be known to both the sender and the receiver that the shared. The complexity with this approach is the distribution of the key. Symmetric key cryptosystem schemes are usually categorized such as stream ciphers or block ciphers. Stream ciphers work on a single bit (byte or computer word) at a time and execute some form of feedback structure so that the key is repeatedly changing.

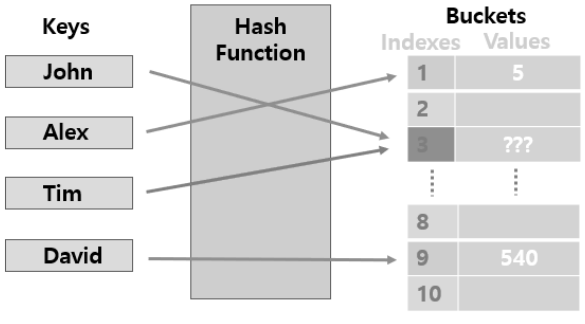


- **Asymmetric Key:** Asymmetric cryptosystem is a second form of cryptosystem. It is called Public-key cryptosystem. There are two different keys including one key is used for encryption and only the other corresponding key should be used for decryption. There is no other key can decrypt the message and not even the initial key used for encryption. The style of the design is that every communicating party needs only a key pair for communicating with any number of other communicating parties. Asymmetric cryptosystem is scalable for use in high and ever expanding environments where data are generally exchanged between different communication partners. Asymmetric cryptosystem is used to exchange the secret key to prepare for using

symmetric cryptosystem to encrypt information. In the case of a key exchange, one party produce the secret key and encrypts it with the public key of the recipient. The recipient can decrypt it with their private key. The remaining communication would be completed with the secret key being the encryption key. Asymmetric encryption is used in key exchange, email security, Web security, and some encryption systems that needed key exchange over the public network.

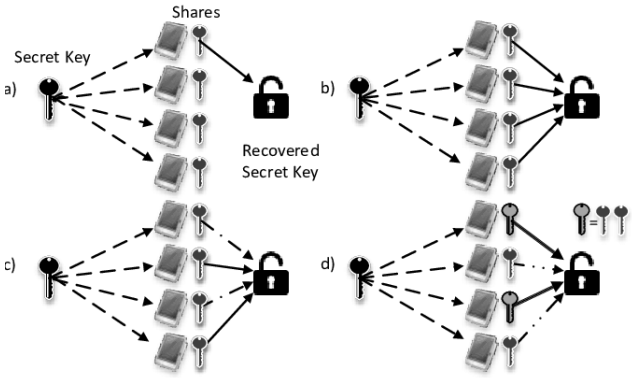


- **Hashing:** Hashing is the process of transforming any given key or a string of characters into another value. This is usually represented by a shorter, fixed-length value or key that represents and makes it easier to find or employ the original string. The most popular use for hashing is the implementation of hash tables. A hash table stores key and value pairs in a list that is accessible through its index. Because key and value pairs are unlimited, the hash function will map the keys to the table size. A hash value then becomes the index for a specific element. A hash function generates new values according to a mathematical hashing algorithm, known as a hash value or simply a hash. To prevent the conversion of hash back into the original key, a good hash always uses a one-way hashing algorithm.



Hash Collision

- **Secret Sharing:** Secret Sharing refers to cryptographic methods for taking a secret, breaking it up into multiple shares, and distributing the shares among multiple parties, so that only when the parties bring together their respective shares can the secret be reconstructed. More specifically, the holder of a secret, sometimes referred to as the dealer, creates n shares of a secret and defines a threshold t for the number of shares that are required to reconstruct the secret. The dealer then proceeds to distribute the shares so they are controlled by different parties. In secure secret sharing schemes, an attacker that gains access to fewer shares of the secret than defined by the threshold gains no information about the secret. Secret sharing schemes are useful because they allow for more secure storage of highly sensitive data, including encryption keys, missile launch codes, and numbered bank accounts. By distributing the data, there is no single point of failure that can lead to its loss.



6. Conclusion

This paper gives detailed information about what cryptosystem and various Cryptosystem techniques to encrypt and decrypt the data are. Cryptosystem is used in all fields to secure data and prevent it from getting hacked. For example- for securing passwords, authenticating banking transactions, etc.

Nowadays, various new cryptographic techniques are developed and cracked; hence, it is important always to be aware of computer threats and take precautions to avoid them as best as we can.

REFERENCES

- Quantum Cryptosystem and the future of cyber security by Nirbhay Kumar Chaubey and Bhavesh Prajapati
- https://www.tutorialspoint.com/
- https://www.educba.com/