IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 12, Issue 1, December 2021
Impact Factor: 5.731

A Review Paper on Cryptography and Network Security

Disha Satyan Dahanukar and Durva Sanjay Shelke
Department of Computer Engineering
Shri Bhagubhai Mafatlal Polytechnic, Mumbai, Maharashtra, India
dishadahanukar@gmail.com and durvashelke09@gmail.com

Abstract: *With the explosively growing internet that has been merging with our lives for the past few decades, data and network security has been of utmost importance as society moves towards the age of digital information. As the number of users connected to the web increases, the threat faced by the network because of attackers also increases. Cryptography, the science of information security derived from the inherent needs of humans to converse and share information or communicate selectively at times, has the primary function of sending correct data over the network without any undesirable modifications. In cryptography, the original message is masked or encrypted by the sender and has to be decoded or decrypted by the receiver using a predefined set of algorithms decided before the commencement of the data transmission. Thereby, successfully avoiding redundant people from accessing or understanding the message as it is converted to content unreadable by the human eye.*

Keywords: Cryptography, Encryption, Decryption, Security.

I. Introduction

[1] Due to the growing safety concerns with the pandemic, contactless lifestyle with the help of digitalization has been getting a boost now more than ever. Increasing convenience through online services such as e-commerce, e-mail, e-banking, e-schools, e-records, etc. increases the threat of cyber-attacks by illegal users through trojan horses, backdoor viruses, fake websites and emails. The security of the information and network is not compromised by the study of secure communication. One of the most reliable ways is using Cryptography whose historical roots date back to 2000 B.C. The Greek term Cryptography, originated from 'Krypto' meaning hidden and 'graphene' signifying writing, is the art and science of concealing messages with images, symbols, numbers or alphabets. Here, data is encrypted using the security key which is known only to the respective sender and receiver. Keys can be of two types namely, symmetric key and asymmetric key. Cryptographic goals that are access control, authentication, confidentiality, data integrity and non-repudiation play a major role in modern cryptography. Even though cryptography is extremely useful, it is also considered highly brittle, as cryptographic systems' reliability can be compromised due to a single programming or specification error. [3]

CIA Triad is another important concept in cyber security. It stands for confidentiality, indicating only the authorized information is trustworthy and accurate and lastly, availability, meaning that authorized users have access to the systems and the resources they need.

II. Important Components Of Cryptosystem

[2] Cryptography is the process of transforming the secret data or information into an unreadable or scrambled form. Execution of cryptographic techniques and their associated transportation providing security services is known as a cryptosystem or cipher scheme. The various mechanisms of a basic cryptosystem are as follows

(a) Plain text: The initial message or information that we want to send secretly.

(b) Cipher text: It is the scrambled or unreadable form of the initial information or message.

(c) Key: It is the rule used to scramble or unscramble the data.

(d) Encryption Function: It is the method using which the cipher text is generated.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 12, Issue 1, December 2021
Impact Factor: 5.731

(e) Decryption Function: It is the inverse of encryption. It is generation of the original message on the receiver's end.
(f) Encryption Key: The encryption key is inputted in the encrypted algorithm by the sender along with the plaintext to calculate the ciphertext.
(g) Decryption Key: The decryption key and encryption key share a connection but are not identical all the time. In order to compute the plaintext, receiver inputs the decryption key into the decryption algorithm along with the ciphertext.

III. HISTORY

The origin of cryptography or secretive writing can be dated back to the birth of the writing system of humans. As time went by, with evolution in mankind; groups, tribes and kingdoms came into being. This gave rise to power and political conflicts and the need to have confidentiality in the sent messages between kingdoms.
[2] [5] Hieroglyph is a 4000-year-old technique developed at the beginning of secretive writing in Egypt where the messenger who would carry the message on the king's behalf was the only person with the key needed to decrypt the message. Following are a few of the historic cryptographic algorithms.

3.1 Caesar Cipher

[1] Julius Caesar invited the Caesar cryptography style in the Gallic Wars. This is the most basic type of cryptographic algorithm used which replaces the plain text alphabet to an alphabet 3 letters ahead of it. For the alphabets, A, B and C; X, Y and Z are used as a representation. As the algorithm only uses a shift of 3 alphabets, decrypting it is a no-brainer in today's time; but, when it had been developed during the war in historic times, Julius Caesar could successfully maintain the confidentiality of the message.[2]

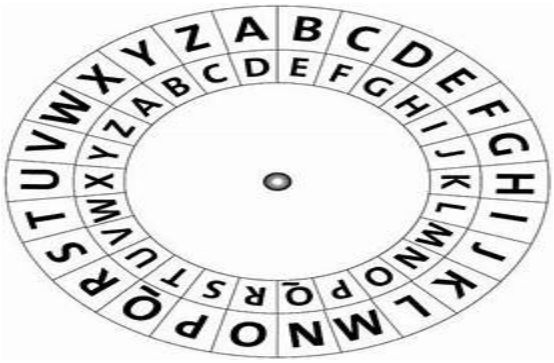

Figure 1

3.2 Simple Substitution Ciphers

[1] Simple substitution cipher also known as the monoalphabetic cipher is a technique of writing alphabets in order and alphabets in a random sequence beneath each of the ordered alphabet, the plaintext in this type of algorithm is always replaced by the letter beneath it to create ciphertext. [2]

Plain text	a	b	c	d	e	f	g	h	i	j	k	l	m
Cipher text	N	O	A	T	R	B	E	C	F	U	X	D	Q
Plain text	n	o	p	q	r	s	t	u	v	w	x	y	z
Cipher text	G	Y	L	K	H	V	I	J	M	P	Z	S	W

Figure 2

3.3 Ceaser Shift Ciphers

[1] The roman technique of cryptography associates an English letter (a - z) with numbers (0-25) and performs encryption and decryption accordingly. The word in the plain text will be substituted by its corresponding number and a number decided on as the key will be added to the previous series of numbers to finish encryption. The same key will

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 12, Issue 1, December 2021
Impact Factor: 5.731

be used by the receiver to decrypt and understand the message initially sent. This algorithm has the shortcoming of being easily decrypted as only 25 shifts are possible for each alphabet other than itself and the number for the key used throughout the message encryption is the same.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Figure 3

3.4 Transposition Ciphers

[1] The letters of plain text are altered using specific key and rules. It has 2 types namely, complete columnar transposition and incomplete columnar transposition. In both these types, a rectangular box whose width is equal to the length of the word in the message is used. The number of rows used to encrypt the message is dependent on the requirement of the message. In the complete columnar transposition method, each of the columns has the same length as when the plain text is written, all the empty places in the column are filled with null values. On the other hand, in incomplete columnar transposition, the length of the columns can vary as no null values are used making the ciphertext more difficult to be decrypted without the key.

4	3	1	5	2
N	A	T	S	R
I	S	P	T	O
X	N	I	X	O

Plain text: TRANSPOSITION
Keyword: 43152
Ciphertext: NI

Figure 4

IV. ENCRYPTION

[4] Encryption is the process of converting a simple plain text message into a non-understandable message known as cipher text. It is done by using an encryption algorithm. We need encryption to hide a message from others, to maintain confidentiality in the transmitted information. For example: If you and your cousin are at a family function you would prefer talking in a language others wouldn't understand (something you come up on your own). By this you can communicate without worrying that a third person is listening to you and only the receiver knows what the message is. Even if this example is basic, corporate companies will use the same logic on a higher scale so that only the receiver knows the information and others trying to hack or trying to decode the message cannot do it since they don't have the respective key and decryption is not possible without the key. So, encryption is used for confidentiality and integrity. Encryption is done with the help of algorithms and keys. [6]

In encryption, 2 types of keys are used, namely public key and private key.

1. Pubilc key: In this type of encryption one of the two keys being used is kept secret. One is used for encryption and other for decryption.
2. Private key: In this type of cryptography only one key is used. The sender and receiver share the same key. As the same key is shared by the sender and receiver, it is faster than public key cryptography.

Encryption can be further subdivided into symmetric encryption and asymmetric encryption:

4.1 Symmetric Encryption

[4] It is the simplest kind of encryption since the same key (private key) is used to both encrypt and decrypt the message. Both, the sender and receiver should know the secret key also known as the shared key to encrypt/decrypt the message. The user can change the meaning of the message by changing the key since same key is used. It is called symmetric cryptography since same key is used at both ends (encryption and decryption). AES 256 and AES 128 are the most widely used symmetric algorithm but a few other examples include blowfish, DES, AES, RC4, RC5, RC6 etc.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 12, Issue 1, December 2021
Impact Factor: 5.731

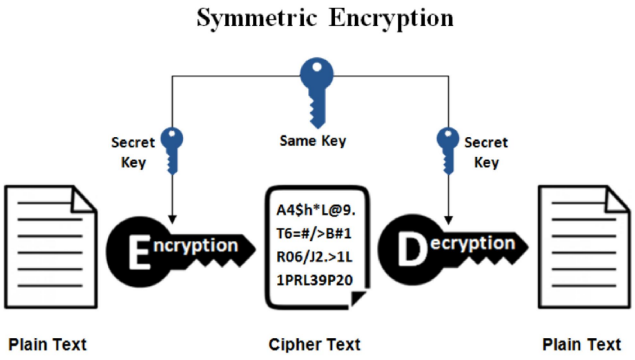

Figure 5

4.2 Asymmetric Encryption

[4] In these two keys are used where one is public while the other one is private. Hence, it is also known as public key encryption. The message encrypted with the help of public key is decrypted with the help of private key. The public key is available to everyone and they can encrypt a message to send it, the second key is kept private so that only the receiver has its knowledge. Most common application of the public key is every web server on the internet providing secure purchase. User's transaction is encrypted without give and take of a private key. This is a part of the background process. Public key encryption is the backbone of the widely used E-commerce platform today.

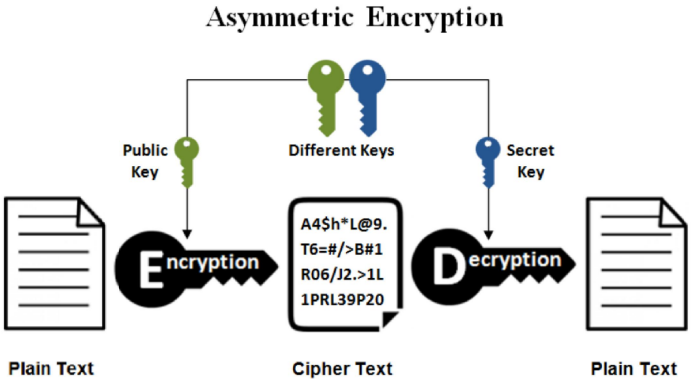

Figure 6

V. Decryption

[4] Decryption is the reverse of encryption. It is the process of converting a cipher text to understandable message. Key plays an important role as decryption of the cipher text is only possible by the use of the correct key on the receiver's end. One can only decode a message with the help of the key. Only the receiver should have the knowledge of the key to achieve the basic goal of maintaining confidentiality. It may be same as the one with the sender or a different one depending on the type of encryption. Decryption cannot be performed with an incorrect key.

VI. Modern Algorithms

As we already saw previously, cryptographic algorithms can be divided into symmetric and asymmetric algorithms. Following is a short introduction to these algorithms and some of its applications.

6.1 Symmetric Algorithms

1. DES - DES or data encryption standard was introduced in 1970. Its main purpose is to encrypt and decrypt a message. The key size in DES is 56 bit which performs encryption on a block of size 64 bit. 3DES, a variant of DES, as the name suggests is 3DES performed thrice on a block of data. 3DES is slower than DES.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 12, Issue 1, December 2021
Impact Factor: 5.731

2. AES - AES, also known as advanced encryption standard, is an advanced version of 3DES. This algorithm, developed by two cryptographers Joan Daemen and Vincent Rijmen, is different from other algorithms due to its variable key sizes i.e., 192, 256 and 128bits for higher security. [2]

6.2 Asymmetric algorithms

1. RSA - Rivest, Shamir and Adleman introduced an algorithm named RSA. This algorithm is mainly used for transferring of keys in an insecure channel. It is used in electronic industry for online money transfer. Being an asymmetric algorithm, it contains two keys one public known to all and the other private known only to the authorized person. It is a perfect example of CIA triad
2. EIGamal - This algorithm introduced by Taher EIGAMAL in 1985, is an alternative to RSA algorithm. It is used in digital signature scheme. Paillier, named after its inventor Pascal Paillier and used for its semantic security is a homomorphic algorithm.
3. ECC - Elliptic curve cryptography, introduced in 1985 by Neal Koblitz and Victor Miller, is used for encryption, random pseudo generators, digital signatures etc.[2]

VII. SECURITY SERVICES

The CIA triad is the most important module in security. The letters 'CIA' stand for confidentiality, integrity and availability. When all these security objectives are met in an organization then its security profile is stronger to handle any threat.

Figure 7

[5] Cryptography has been developed since the ancient times to make the transmitted information secure. The following are the CIA and other security services which help cryptography achieve its primary purpose:

7.1 Confidentiality

[3] Confidentiality is the security service which keeps the data out of reach of unauthorized access. Confidentiality maintains the privacy and secrecy in the network. An organization wants to keep its sensitive information confidential i.e., Private. This sensitive information is known and accessible only to people who are authorized. This is an important factor to maintain confidentiality. Confidentiality breach occurs by direct attacks like man-in-the-middle and packet sniffing to gain credentials, when the employee is insidious and even at times unintentional due to human error (if the password is not strong enough).

The simplest way of achieving confidentiality is by using secure physical setup and its complexity can go up to the use of arithmetic algorithms for encryption of the information being transmitted over a network. Methods used to ensure confidentiality are account number or token number when banking online, even OTP. Data encryption is the most

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 12, Issue 1, December 2021
Impact Factor: 5.731

common. Other methods are biometric, security tokens, etc. Two factor authentication is a method being implemented now a days in which instead of one we need two passwords while logging in and hence it is more secure.

7.2 Data Integrity

[3] Integrity in other words means incorruptibility. It is the safety service which helps in identification of any undesired alteration made to the data by an illegal entity either intentionally or accidentally. It involves maintaining the accuracy of a message, that is, the message should not be tampered or altered in its lifetime. It means that the message sent from one person to another is same. It can be checked with the help of hashing algorithms MD5 and SHA1. Other methods include digital certificates, digital signatures, non-repudiation. For example: If you send emails with digital signatures attached to them in your organization or to the client's organization, then you cannot deny sending or receiving an email when your digital signature is attached to it. Data integrity is crucial from e-commerce and business websites. (Simplest example being when talking on phone if the sender receives a message a bit different than what you said because of the surrounding noise it can lead to misunderstandings.) This service helps in confirming whether the data is whole since the authorised user created, transmitted or stored the data. Even though data integration cannot prevent the modification being made to data, it can detect illegal manipulation.

7.3 Authentication

[5] Recognition of the origin is provided by authentication. It is a confirmation for the receiver that only a recognised and established sender is sending the data. Message authentication is the first variant of authentication and identifies the creator of that data/message without any regard for the in-between transmission points such as router or scheme. The second variant of authentication is the entity authentication which says that the data has been sent from a confirmed source/entity. Apart from these two main authentication parameters others like date and time of transmission or creation of data are also included.

7.4 Non-repudiation

[3] This type of security service ensures that entity does not refuse its previous commitment, possession or action related to the data. It means that there is a proof of message being sent from one person to another and they cannot deny that action. It is important so that one is accountable for his/her action and cannot deny doing it.

It is a security repair that guarantees the transmission and formation of the said data to a recipient or third party is not denied by the original creator of the information. Non-repudiation plays a very important role in cases where a conflict over exchange of data is likely to arise. Examples can be when an order has been placed online neither the purchases nor the service provider can deny the purchase order if non-repudiation was enabled during the transaction.

It can be ensured by account logging and monitoring the login activities of a person i.e., where he/she has logged at what time and what are the things done. Digital signatures verify an individual's identity so if you are sending a mail with digital signature attached to it you cannot deny that you have sent it. Read receipts confirm that the person has received the message and records the time.

7.5 Availability

[6] Availability is also a security service which ensures the constant availability of resources and services to the authorized party. Availability is ensured by fast and adaptive disaster recovery, less down time during upgrades and backup, data backup, redundancy and redundant system. Firewalls and proxy servers can guard against downtime and unreachable data blocked DOS attack (denial of service). All the updates should be done time to time, having data backups ensures that if something happens you have a copy of your data to restart and keep the business going.

Example: Netflix expects its services to be available to the user all the time (99.99%). Which means that 99.99% of the time users should be able to access Netflix.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 12, Issue 1, December 2021
Impact Factor: 5.731

VIII. CONCLUSION

As the internet grows, the field of cryptography also grows continuously to provide more secure information transmission to all the users connected all over the world. As we face a constant threat of data integrity being at a risk, organizations consider confidentiality as a vital factor. Cryptography promises a robust, safe and strong network security along with data security. Therefore, development of a secure network for a firm's needs helps the network refrain from the risks it can face in an operational environment. Cryptography continues to emerge as the most powerful medium in the IT industry to provide privacy in e-commerce, medical, personal and financial data. A reliable security policy should ensure data or information confidentiality and authentication with no effect on its availability or integrity.

REFERENCES

[1]. Abdalbasit Mohammed Qadir and Nurhayat Varol "A Review Paper on Cryptography" in 7th International Symposium on Digital Forensics and Security (ISDFS), June 2019.

[2]. Dr. R.K Gupta "A Review Paper On Concepts Of Cryptography And Cryptographic Hash Function" European Journal of Molecular & Clinical Medicine, ISSN 2515-8260, Volume 07, Issue 07, 2020

[3]. Dr. Sandeep Tayal, Dr. Nipin Gupta, Dr. Pankaj Gupta, Deepak Goyal and Monika Goyal "A Review paper on Network Security and Cryptography", Advances in Computational Sciences and Technology, ISSN 0973, 6107 Volume 10, Number 5, pp. 763 – 770, (2017).

[4]. Faiqa Maqsood, Muhammad Ahmed, Muhammad Mumtaz Ali and Munam Ali Shah "Cryptography: A Comparative Analysis for Modern Techniques", International Journal of Advanced Computer Science and Applications (IJACSA), Vol. 8, No. 6, 2017.

[5]. Preeti Dewangan "A Review Paper on Network Security and Cryptography", International Journal of Science and Research (IJSR) ISSN: 2319-7064, Volume 9 Issue 1, January 2020

[6]. Mitesh Sharma, Review on Cryptography in Network Security, ETRASCT – 2014 (Volume 2 – Issue 03), IJERT, 30-07-2018