iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** II **Month of publication:** February 2022

DOI: https://doi.org/10.22214/ijraset.2022.40401

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue II Feb 2022- Available at www.ijraset.com

Cryptography: A Brief Review

Milind Kaushal[1]
[1]*Department of Computer Science and Engineering, Harcourt Butler Technical University, Kanpur*

Abstract: ***This paper reviews the concept of cryptography and some of the cryptographic algorithms. It discusses the importance of cryptography and how it is useful in the data security world. The history of this concept goes way back and has found uses in the times of wars. It has become way more advanced and complicated than it used to be but is still not perfect.***
Keywords: Cryptography, Asymmetric Cryptosystem, Cipher text, Encryption Algorithm, Diffie-Hellman, DES, 3DES

I. INTRODUCTION

With everything gone online, there comes a lot of risks. Cyberattacks like phishing, DDoS put out a very grave danger to the things on the internet. One of the classifications of such attacks is middleman attacks where the network is intercepted by a third party known as the attacker to gain all the information packets being sent from the connection. To prevent such attacks, there exists a concept in Cyber Security; Cryptography.

II. LITERATURE REVIEW

Cryptography is a technique to achieve confidentiality in messages and data. Abdalbasit Mohammed Qadir et al. [1] explain how it is applied at a higher level nowadays and nobody is even aware of using it. It is a very ancient technique that is still in the process of being evolved. As pointed out by Susan et al. [2] the crackers always come up with new ways of attacking a machine and networks which leads to the creation of new courses to prevent those types of attacks in the future. Network and computer security is a new and fast-moving technology. These security courses mainly focus on algorithmic and mathematical concepts like hashing techniques and encryption. Sandeep Tayal et al. [3] discuss how the emergence of social media and commerce websites brings to light a major issue with information security; the generation of huge amounts of data and their transfer over the network in a secure way. This is where cryptography and its methods come into play and become of high importance. This paper brings up different methods that networks use for encryption and securing data transfer.
Anjula Gupta et al. [4] show how information security has become a challenge in the field of computers and networking. This paper also discusses the different asymmetric methods of encryption used to encrypt and secure data.
Studied by N. Varol et al. [5] are the symmetric encryption methods in which the content to be encrypted is first converted into a cipher that isn't understood by the algorithm. Generally, this is used for text and speech content.
As far as the goals of cryptography are concerned, James L. Massey [6] discusses the existence of two main goals that cryptography aims to achieve as they are: authenticity and/or secrecy.

III.CRYPTOGRAPHY: THE CONCEPT

The main motive of cryptography is to ensure confidentiality of the data when being transferred over some channel, such as the internet, or ensuring that if accessed by an unauthorised person, it doesn't make sense to them at all.
The data to be sent is commonly termed as "plain text" and is converted to some kind of gibberish. This process is known as "encryption" and is achieved using methods called "encryption algorithms" which require an extra piece of information i.e. the "encryption key". The receiving end then converts the cipher text to plain text using a method known as "decryption" which requires the "decryption key".

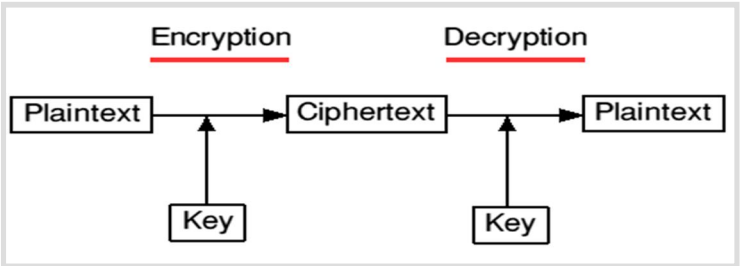


Fig. 1 Cryptography Methodology [7]

©IJRASET: All Rights are Reserved

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue II Feb 2022- Available at www.ijraset.com

IV. HISTORICAL ALGORITHMS

Cryptography can be dated back to as early as the 19th century. This section deals with the earliest cryptographic algorithms that were used long before the concept of public-key was introduced.

A. Caesar Cipher

This is one of the earliest ciphers invented by Julius Caesar. Julius Caesar was the emperor of Rome who devised this to use in wars. The way this worked was all the alphabets of the English letter were shifted by 3 places and thus resulted in the cipher text. To break it, all one needed to do was shift the alphabet back 3 places. Though this was very easy to break, it was very useful in wars in ancient times.

Now also a shift algorithm is often regarded as Caesar Cipher. There is a shift of three in this method but the number could range between 1 to 25.



Fig. 2 Caesar Wheel [8]

B. Simple Substitution Cipher

Also known as the Monoalphabetic Cipher, it is exactly what the name suggests. For the encryption, every alphabet is replaced with the random letter that it has been assigned according to the substitution table. For decryption, it is exactly the opposite.

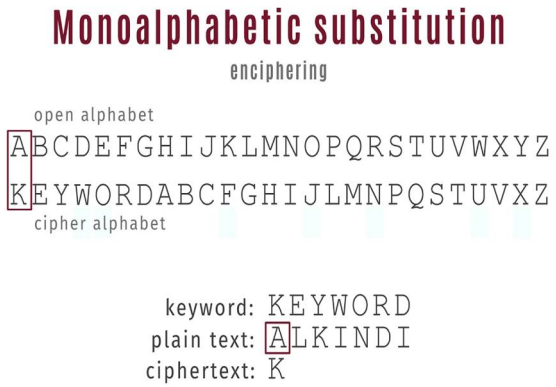


Fig. 3 Substitution Cipher Table [9]

V. MODERN ALGORITHMS

After the introduction of the “Public Key” , the algorithms have been classified into three main categories:

1) Cryptographic Hash Functions
2) Symmetric Encryption
3) Asymmetric Encryption

©IJRASET: All Rights are Reserved

A. Symmetric Encryption

This type is the one which uses only a single key for the process of encryption and decryption. Both parties involved in a symmetric exchange, require the exchange of the key for the decryption of the message. The encrypted message is not readable by a third party and the key when received by the recipient, reverses the algorithm and converts the cipher text to plain readable text.

These are also of two types: Block (DES, 3DES, AES etc.) and Stream (RC4, RC5 etc.)

1) *DES:* Based on the Fiestal block cipher, called LUCIFER, Data Encryption System (DES) was developed by IBM in 1971. It uses symmetric encryption method to convert 64-bit blocks to cipher text using 48-bit keys.

It follows the given steps:

a) The process begins with the 64-bit plain text block getting handed over to an initial permutation (IP) function.
b) The initial permutation (IP) is then performed on the plain text.
c) Next, the initial permutation (IP) creates two halves off the permuted block, referred to as the Left Plain Text (LPT) and the Right Plain Text (RPT).
d) Each LPT and RPT goes through 16 rounds of the Fiestal Structure using a different key every time.
e) Finally, the LPT and RPT are rejoined and a Final Permutation (FP) is performed on the newly combined block.
f) The result of this whole process produces the desired 64-bit cipher text.

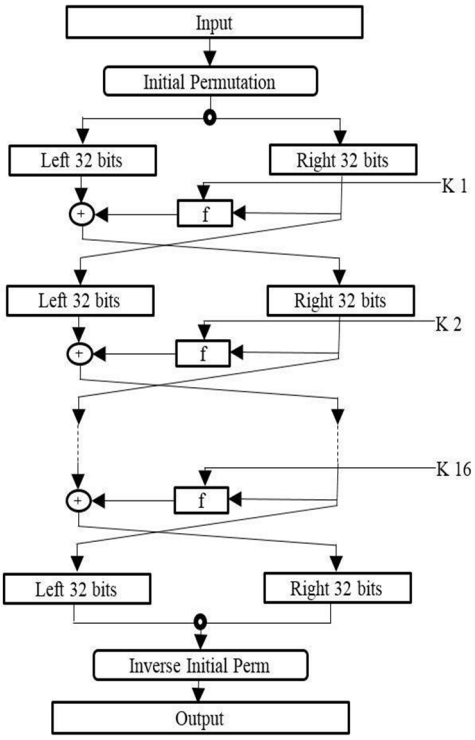


Fig. 4 DES Algorithm Chart [10]

2) *3DES:* It is an enhanced version of the DES algorithm. It is more reliable as it makes use of a key of length 192 bits. The key is first divided into 3 parts of 64-bits. The rest of the procedure is the same as that of the DES. The only difference is that the first key is used to encrypt the data and the second one to decrypt. Then the third key encrypts the data finally.

B. Cryptographic Hash Functions

These are also referred to as Pseudo Random Functions (PRF). It takes as an input a variable length string and produces a fixed length hash after the application of a hash function. A hash function must have the following properties:

1) It must be non-invertible.
2) It must be completely collision resistant i.e it must be impossible to find two different inputs that produce the same hash value

The following collision resistances are possible:

a) Pre-Image Resistance: If given is a hash value h, a message m should be difficult to find for which h = hash (m). If a function doesn't satisfy this property, it becomes vulnerable to pre-image attacks.

b) Second Pre-Image Resistance: If given a message m1, then another random message m2 should be difficult to find for which hash(m1) = hash(m2). If this function doesn't satisfy this property, it becomes vulnerable to second pre-image attacks.

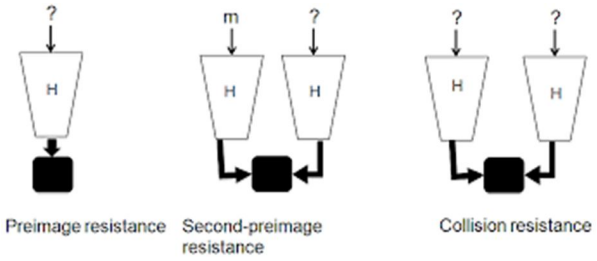


Fig. 5 Different Collision Resistances [11]

C. Asymmetric Encryption

The question that gets asked quite often is regarding the use of asymmetric encryption which is because of the already existent symmetric algorithm. Well, as we know, symmetric exchange uses a single key for both encryption and decryption and if this were to be accessed by a third party, the data would get breached. This is where the asymmetric encryption comes in handy. It uses two separate keys for encryption and decryption; public key for the former and private key for the latter. The multi-key system proves to be a clever and secure way to exchange the key between the two parties involved. Basically how it works is, both the keys belong to the recipient. The sender encrypts the data using the recipient's public key and sends the data over to the receiver who then decrypts it using the private key.

Also known as Public Key Cryptography due to its open nature, this type can be found to be playing a very significant role in various networking and internet concepts such as Digital Signatures, TLS/SSL Handshake to name a few.

A few examples of algorithms that use asymmetric encryption include Diffie Hellman, DSA, RSA etc. This next section discusses the Diffie Hellman key exchange in detail.

VI. DIFFIE-HELLMAN KEY EXCHANGE

This, as the name suggests, was devised by Whitfield Diffie and Martin Hellman in the 1970s. It is very useful in the scenario when the recipient and the sender do not have way to pre-decide a code or a key before the encryption.

So, the working of this algorithm is very mathematical but in layman terms, it is explained using a very famous colour analogy.

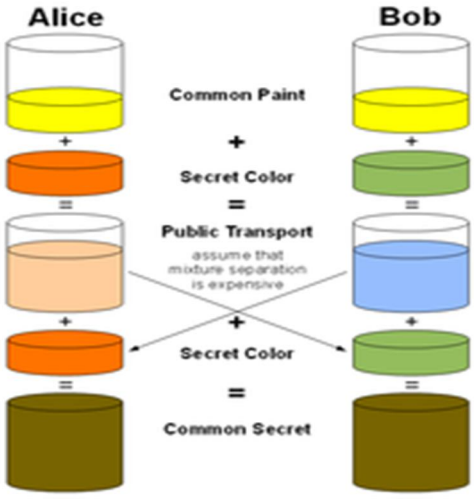


Fig. 6 Diffie-Hellman Key Analogy [12]

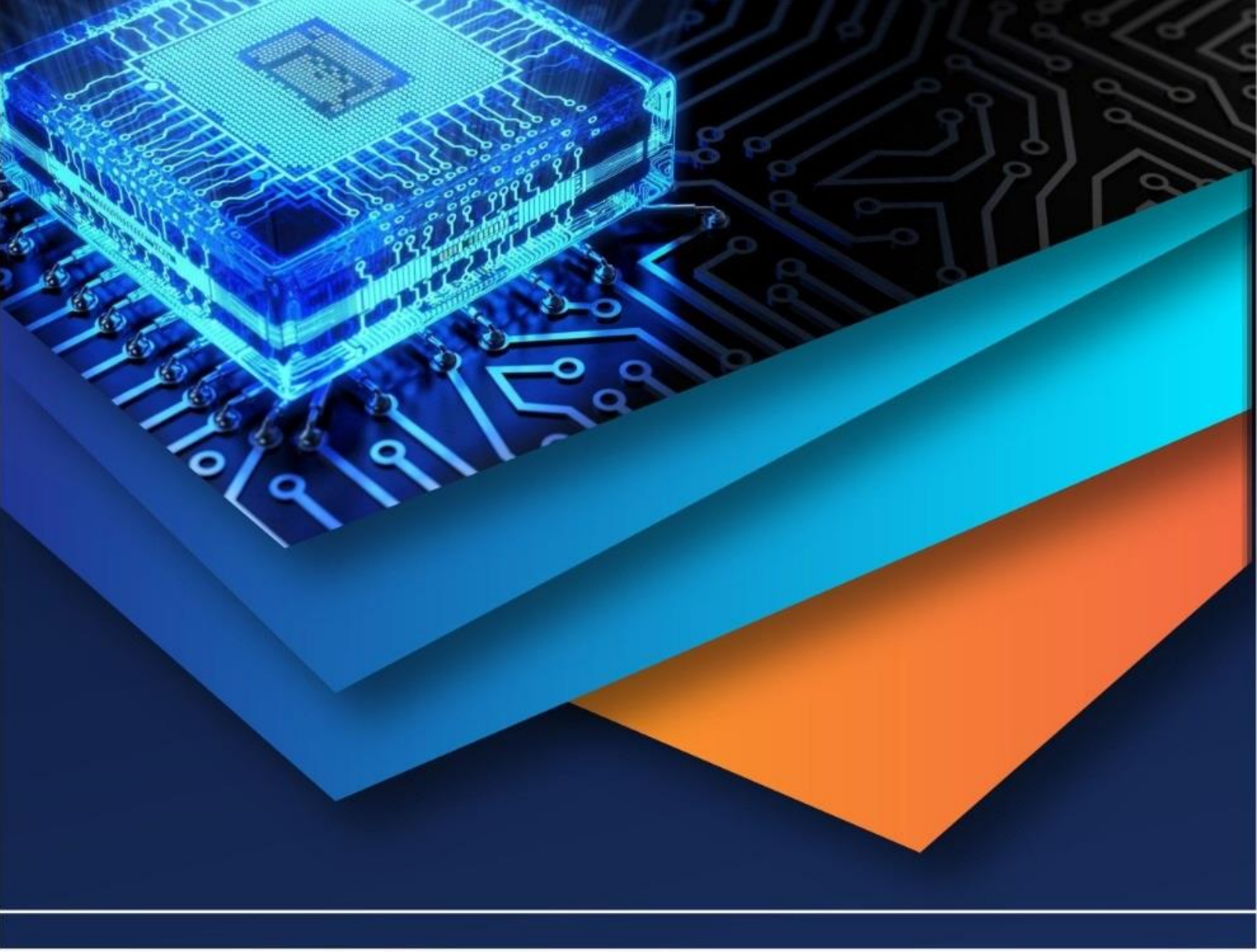
Let there be two people Alice and Bob. They decide on a common colour, for our example let it be yellow. Now both Alice and Bob decide on a secret colour of their own which only they know about. Now, they add their colours in the common colour and end up with a light orange-ish colour for Alice and a blue for Bob. This is what they send to each other in the open. Even if this is intercepted by a third person, it would be of no use to them as nothing is known to the third person. Now after the exchange Alice has the blue and Bob has the orange mixture. Now they again add their secret colours to the mixture they have in possession. After this they both end up with the same brown colour. This shared colour is known as the common secret.
The gist of this is that they successfully exchanged and ended up with the same product in a secure way.

VII. CONCLUSION

The primary aim of security tech is to achieve confidentiality, integrity, availability and non-repudiation and cryptography aids in getting to them. Cryptographic algorithms help in establishing a secure channel and connection for the transfer of data and information between two entities. Cryptography is an ever emerging field in the IT world. With the world becoming more tech centred and everything going digital, data security and hence cryptography have become more important than ever.

REFERENCES

[1] Mohammed, Abdalbasit & Varol, Nurhayat. (2019). A Review Paper on Cryptography. 1-6. 10.1109/ISDFS.2019.8757514.
[2] S. J. Lincke and A. Hollan, "Network Security: Focus on Security, Skills, and Stability," in 37th ASEE/IEEE Frontiers in Education Conference, Milwaukee, 2007.
[3] S. Tayal, N. Gupta, P. Gupta, D. Goyal and M. Goyal, "A Review paper on Network Security and Cryptography," Advances in Computational Sciences and Technology , vol. 10, no. 5, pp. 763- 770, 2017.
[4] A. Gupta and N. K. Walia, "Cryptography Algorithms: A Review," INTERNATIONAL JOURNAL OF ENGINEERING DEVELOPMENT AND RESEARCH, vol. 2, no. 2, pp. 1667-1672, 2014.
[5] N. Varol, F. Aydoğan and A. Varol, "Cyber Attacks Targetting Android Cellphones," in The 5th International Symposium on Digital Forensics and Security (ISDFS 2017), Tirgu Mures, 2017.
[6] J. L. Massey, "Cryptography—A selective survey," Digital Communications, vol. 85, pp. 3-25, 1986.
[7] https://ehindistudy.com/wp-content/uploads/2015/10/wpid-au265a.gif
[8] https://www.boxentriq.com/img/caesar-wheel.png
[9] https://i.ytimg.com/vi/Dz1RW_W2zGI/maxresdefault.jpg
[10] Mushtaq, Muhammad & Jamel, Sapiee & Disina, Abdulkadir & Pindar, Zahraddeen & Shakir, Nur & Mat Deris, Mustafa. (2017). A Survey on the Cryptographic Encryption Algorithms. International Journal of Advanced Computer Science and Applications. 8. 333-344. 10.14569/IJACSA.2017.081141.
[11] https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcSc-m-feNAqXH-URl3g21OKSva0NSXD8RGrl9zH1-b8mzyxh5VvvoKFoSaVgqpoK_RVAG0&usqp=CAU.
[12] https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)