02 Days, 5th International Conference on Recent Trends In Engineering, Science & Management
Parvatibai Genba Moze College of Engineering, Wagholi, Pune (ICRTESM-16)
9th-10th December 2016 , www.conferenceworld.in ISBN: 978-93-86171-12-2

A STUDY OF MATHEMATICAL CRYPTOGRAPHY – THE PART OF MODERN ERA

Prof. S.P. Waghmare[1], Prof.V.N. Agme[2]

[1,2]Bharti Vidyapeeth College of Engg. Kharghar ,Navi Mumbai (India)

ABSTRACT

Cryptography is the mathematical application in todays modern era playing an important role in the field of security like transmission & receiving of confidential data between sender & receiver. The current paper is presented as a survey of cryptography its role, its application & how valuable tool it can be in various sectors like Military security, Defence Services, e-commerce, Nation's secured data, business transaction, internet payment system. Now a day it has become a backbone of national security, networking system& e-commerce. Various cryptography algorithms are channeled by the encryption & decryption, so it ensures that the data should be sent to the authorized person without any modification or editing. Only authorized person is able to get the details about the data.

Keywords: Cryptography, Encryption, Decryption, Cipher Text, Plain Text, data, Defense Services.

I INTRODUCTION

The main context of the encryption/decryption program implementation is the creation of encryption key. Now a day, crystography has many commercial uses. If we are protecting secret information then cryptography is needed at high level of privacy of individuals and groups. However, the main purpose of cryptography is used not only to provide secretly, but also to give solution for other problems like: data integrity, authentication, non-repudiation[1].

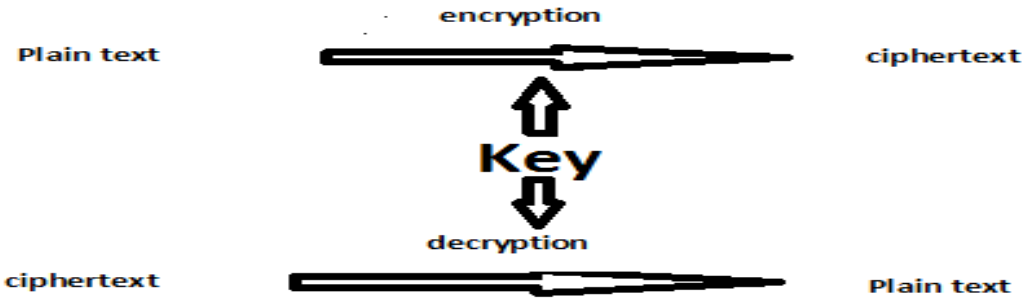
Cryptography is the ways that allow information to be sent in a secure form in such a way that only receiver is able to regain this information. Presently continuous researchers on the new cryptographic algorithms are going on. However, it is a very difficult to find out definite algorithm, because we have already known that they must consider many factors like: security, the features of algorithm, the time complicacy[2]. Cryptanalysis is called attackers in the field. There are two kinds of Cryptography in the world, one which will encrypt data and secure it from your young sister, second which will encrypt data and Security from a job government.

1.1 History of cryptography

Providing security and protecting data has become a very difficult task. Every organization today must have policies related to data safety. To do this certain algorithms tools should be carry out. Cryptography usually called" Code breaking" exists from ancient days. Most of it was used during wars to send messages in hidden layout. In fact, the cryptography word comes from the Greek Words Kryptos and graphein which means hidden & writing respectively[3]. It mainly deals with algorithem.the first recognized application of cryptography is originated in non-standard hieroglyphs curved into monuments from old kingdom of Egypt circa 1900 B.C. It was created in such a way to send messages in coded format & would be easy for the receiver to read it who knows to decode it. In the sixth century B.C., contained of curving a roll of paper around a cylinder & then marking the messages on paper. The unrolled paper was then send to recipient, who could easily decode the message if he know diameter of the cylinder. 2000 year ago Julius Caesar used a switch over numeric characters, recognized or known as caser cipher Roger Bacon characterized no. of ways in 1200s[4]. We have two of the best offering from this civilization. One of them is still in use called this type as "Nirabhasa", in which joints of fingers represents Newels & other parts as consonants**.** The part of Indian civilization in ancient time is that answerable for first relation in recorded history for the use of crypt analysis for political uses. Though no mechanisms are given for providing such suggestion, there is still cryptographic development seated in the context that such type of crypto analysis could surely be achieved[3]. In simple terms cryptography is the style to convert message(plain text) into tabulated message (encrypt) from sender &covey it to Receives who decrypts the message into readable format (Plain text) After receiving in to avoid the message from getting stolen, damaged or lost & in order to protect it. Cryptography has come up as important tool for data transmission. A lot of algorithms of cryptography have been studied[5].

1.2 Secret key cryptography

In Secret cryptography we have to use single key. A Message in its initial form is called Plain Text or clear text. The Mangled information is called Cipher Text. The process of formation of cipher text from plain text is called Encryption. The Decryption is exactly reverse process of encryption to obtain plain text from cipher text[6].



ISBN: 978-93-86171-12-2

1.3 Encryption& Decryption:

Data that can be read and understood without using a key or special measure is called Plain text or Clear text. The method of disguising plain text in such a manner so that content is hidden is known as Encryption[7]. Encrypting plain text result in unreadable gibberish sentence is called cipher text. Encryption is used to ensure that information is hidden from third party even those who can see the encrypted data[8]. The conversion of cipher text to original plaintext is called Decryption.

Common Targets in cryptography

Cryptography has four main goals. They are:

1. Message confidentiality: Only an authorized recipient should be able to extract the contents of the message from its encrypted form. Resulting from steps to hide, stop or delay free access to the encrypted information.
2. Message integrity: The recipient should be able to determine if the message has been altered.
3. Sender authentication: The recipient should be able to verify from the message, the identity of the sender, the origin or the path it traveled (or combinations) so to validate claims from emitter or to validated the recipient expectations.
4. Sender non-repudiation: The emitter should not be able to deny sending the message.
5. *Key exchange:* The Process by which crypto keys are Common between sender and receiver[9].

For this we can formulate

$$C=E_k(P)$$

$$P = D_k(C)$$

Where P = plaintext, C = ciphertext, E = the encryption method, D = the decryption method, and k = the key[10].

II RESULT

It is modes which use mathematics for encryption and decryption crystallography To Store sensitive information & to transfer it across different network like Internet, so that it cannot be read by any third party other than the intended recipient. Hence Crystallography is a method of securing data also it is a way to analyze and break secure communications, classical cryptanalysis involved a balanced communication of analytical reasoning. It is an application of mathematical tools pattern findings patients' determination and a bit of luck.

The mathematical functions are used in encryption and decryption ciphers or a cryptographic algorithm. Algorithm works in a combination of a word, number, or phase and a key to encrypt plain text. The same plain text is then encrypted to different Cipher texts with the help of different keys. The primary of encrypted data is entirely

dependent on the strength of cryptography and secure of the key. Hence with the help of cryptography loss of major information can be prohibited & is the most secure encryption technique.

III CONCLUSION

After going through the history of cryptography eventually it had proved its enormous roal in the modern age with the help of computer coding, digital algorithm & it is the one of the most advance tool in the security of internet like for the protection of financial transaction for banking shopping then information storage of all retrievals processing & government application. It will also more technically convenient & advance with the safe implementation of complex mathematical equation & protocols.Authors are working on its future aspects.

REFERENCES

1. Nathan Saper, International Cryptography Regulation &the Global Information Economy, Volume 11, Number7, September 2013,see id at 294.
2. Niveditha R,International Journal of Science & Research (IJSR),Volume 3,Issue 4,April2014,ISSN(online):2319-7064.
3. Rajesh R Mane[1],A Review on cryptography Algorithms, attacks &Encryption Tools, International Journal of Innovative Research in computer & Communication Engineering, Volume 3, Issue 9,September2015,
4. Debasis Das1, U. A. Lanjewar2 and S. J. Sharma3, The Art of Cryptology: From Ancient Number System to Strange Number System, Volume 2, Issue 4, April 2013 ISSN 2319 –4847
5. Pranab Garg1, Jaswinder Singh Dilawari2, A Review Paper on Cryptography and Significance of Key Length, IJCSCE Special issue on Emerging Trends in Engineering" ICETIE 2012
6. Vishwa Gupta, Gajendra Singh, Ravindra Gupta, Advance Cryptography Algorithms for improving data Security, International Journal of Advance Research in Computer Science & Software Engineering, Volume 2, Issue 1,Janaware 2012,ISSN:2277128X.
7. Pretty Good,An Introduction to Cryptography,PGP* Version 6.5.1,AS Com Tech AG & Northern Telecom.
8. Bruce Schneier, Jhon Wiley&sons,Applied cryptography Protocols Algorithms & Source Coad in C ,ISBN 0-471-12845-7. & Eli Biham,Adi Shamir,Spinger verlag ,Differential cryptanalysis of the data Encryption Standard,ISBN:0-387-97930-1
9. Mitali,Vijay Kumar,Arvind Sharma, A Survey on Various cryptography Techniqus,International journal of Emerging Trends & Technology in computer Science (IJETTCS),Volume 3, Issue 4,July/August 2014,ISSN:2278 6856.
10. Paull E Gunnells, The Mathematics of cryptography, April 27, 2004● www.math.umass.edu/~ gunnells