*International Journal For Technological Research In Engineering*
*Volume 5, Issue 2, October-2017* *ISSN (Online): 2347 - 4718*

# CRYPTOGRAPHY: A COMPLETE REVIEW

Seema Choudhary[1], Amit Kumar Mishra[2], Jitendra Kumar[3]
[1]M. Tech. Scholar, [2,3]Sr. Lecturer and Head of Department, Computer Science,
[1,2]Sri Balaji College of Engineering and Techology, Jaipur Rajasthan.

***Abstract: Cryptography techniques assumes vital part in picture security systems in correspondence. There are numerous cryptographic algorithms are utilized to shield or conceal secret data from unapproved get to. Encryption is utilized to ensure data in networks in incoherent frame. On the other way, Decryption is utilized to get to indistinguishable frame to unique shape. This paper comprises of examination between four most basic Encryption/Decryption algorithms: DES, 3DES, AES AND BLOWFISH as far as demonstrating these parameters: square size, relationship, entropy esteems, key size, rounds, time utilization and throughput of algorithms. The results demonstrate that Blowfish algorithm is more reasonable than different algorithms for security of classified data.***
***Keywords: Cryptography, Image Encryption, Cipher, Blowfish.***

## I. INTRODUCTION

Giving security and ensuring data has turned into an extremely troublesome undertaking. Each association today should have approaches with respect to data security .keeping in mind the end goal to give security certain algorithms, instruments ought to be actualized. Cryptography frequently called "code breaking" exists route over from old days. A large portion of it was utilized amid wars to send messages in shrouded organize. Truth be told, the very word cryptography originates from the Greek words kryptos and graphein, which mean covered up and composing, separately [1].It is mostly worry with algorithm. The underlying perceived utilization of cryptography is begun in non-standard symbolic representations engraved into landmarks from the Old Kingdom of Egypt around 1900 B.C. It was plan in such an approach to send message in coded design and would be simple for the beneficiary to peruse the message who knows to translate it . The 6th Century BC, comprised of covering a move of paper around a chamber and afterward denoting the message on the paper. The unrolled paper was then send to the beneficiary, who could without much of a stretch disentangle the message in the event that he knew the breadth of the one of a kind chamber [10]. 2000 years prior Julius Caesar utilized a straightforward switch over figure, perceived as the Caesar figure Roger bacon depicted various strategies in 1200s. Blaise de Vigenère distributed a book on cryptology in 1585, and clarified the polyalphabetic substitution figure. In India, mystery composing was in reality more unrivaled, and the administration utilized mystery codes to be in contact with a network of spies spread completely through the nation. We raise two of the remarkable offerings from this human progress. One of them is as yet utilized today, in particular finger correspondences. Old India called this sort of correspondence "nirabhasa", where joints of fingers spoke to vowels and alternate parts use for consonants. The second piece of Indian human progress of old circumstances is that they are responsible for the main reference in written history for the utilization of cryptanalysis for political purposes. Albeit no components are given for completing such recommendations, there is some cryptographic advancement situated in the data that such cryptanalysis could unquestionably e accomplished [9]. In straightforward terms Cryptography is the procedure to change over the message (Plain content) into coded message (encode) from Sender and transmit it to Receiver who converts(decrypt) the message into lucid format(Plain content) subsequent to accepting it to dodge the message from getting stolen, harmed or lost and with a specific end goal to secure it.

## II. TYPES OF ATTACK

### *A. Security Threats*

There are a amount of security dangers that can be the start of a network security assault. Most critical security dangers are dissent of administration, appropriated foreswearing of administration, infections, Trojan steeds, spywares, malwares, unlawful path in to the network property and data, unintentional eradication of the records and the uncontrolled web get to.

### *B. Virus assault*

A computer virus is a program or an executable code that when executed and computer-created, follow up on various undesirable and harming capacities for a computer and a network. Viruses know how to wreck down your hard plates and processors, use memory at a vast scale and wipe out the general execution of a computer or network. A Trojan is a malignant code that performs basic activities yet it can't be duplicated. Trojan is fit for eradicating systems critical records. A computer worm is a program that reproduces to all network and wipe out helpful data. The viruses, malware, adware and Trojan stallions can be controlled on the off chance that you have a modernized antivirus program with the most state-of-the-art design documents.

### *C. Unauthorized Access*

Admission to the network assets and records ought to be enabled just to the endorsed people. Each normal envelope and assets in your network more likely than not been gotten to just by the authorized people and expected to be examined and checked more than once.

### *D. Data stealing and cryptography attacks*

One more risk to a network is loss of the real data and this misfortune can be disallowed, in the event that you utilize

  

great encryption strategies, for example, 128 piece security or 256 piece security encryption techniques. In this way your data when exchanged amid FTP programs, can be scrambled and can't be perused or utilize.

*E. Unauthorized application installations*
An extra virus and security ambush aversion strategy is to introduce just the affirmed programming applications to our arrangement of associations i.e. server and all customer computers. Nobody ought to be allowed to introduce any sort of program which can be wellspring of security dangers, for example, melodies or video programs, gaming programming or extra web based applications.

*F. Application-Level Attacks*
The intruder abuses the restriction in the application layer – for instance, security constraint in the web server, or in flawed controls in the separating of a contribution on the server side. Cases malevolent programming assault (viruses, Trojans, and so on.), web server assaults, and SQL infusion [5].

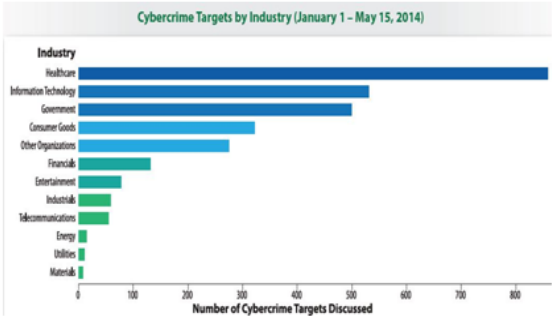


Fig1: Number of Cybercrime Targets Discussed

*2.1 Data Encryption Standard (Des)*
Data encryption standard was the main encryption standard to be distributed by NIST (National organization of standard and innovation). It was outlined by IBM in view of their Lucifer figure. DES turned into a standard in 1974 and it was embraced as a national standard in 1997. DES is a 64-bit piece figure under 56 bit key. There are many assaults recorded against the shortcomings of DES which makes it unreliable piece figure. This standard is open.

*2.2 Triple Des (Tdes)*
The triple DES (3DES) algorithm is considered as a substitution message which gives TDES as a most grounded encryption algorithm which is difficult to break in light of its blends. Two distinctive keys for the algorithm can likewise be utilized which diminishes the memory prerequisite of keys. However, this algorithm has a disadvantage that it is extremely tedious.

*2.3 Advanced Encryption Standard (Aes)*
This algorithm is likewise called as Rijndael which is otherwise called Rain Doll algorithm. It was produced by two researchers Joan and Vincent Rijmen in 2000. Rijndael key and piece length is 128 piece which performs 9 preparing rounds. On the off chance that the bit of the key is expanded preparing rounds are increased consequently. This symmetric square can scramble data of 128 bits utilizing keys 128, 192 or 256. An outstanding assault i.e. Beast compel assault i.e. Savage power assault is the main assault against this algorithm.

*2.4 Blowfish*
This is symmetric piece figure that is successfully utilized for encryption and securing the data introduce in the picture. Bruce Schneier planned blowfish in 1993 as a quick, free algorithm. A variable length key is utilized from 32 bits to 448 bits making it perfect for securing data. This sort of algorithm is sans permit and is accessible free for all clients. No assault is valuable against this algorithm. The rudimentary operations of Blowfish algorithm incorporate table query, expansion and XOR. This algorithm has Feistal rounds. This algorithm has 64 bit piece and is utilized as the swap for DES. This is quick and can encode on 32 bit chip. This algorithm is very reduced. The blowfish algorithm utilized for picture encryption decoding observes up table of Correlation and an Entropy estimation of the algorithm is as appeared in the table beneath.

## III. BACKGROUND THEORY

*3.1. Need of Information Security*
There There are a few methods for ordering cryptographic algorithms. For motivations behind this paper, they will be sorted in view of the quantity of keys that are utilized for encryption and unscrambling, and additionally characterized by their application and utilize. Three sorts of algorithms that will be talked about here.

1. Symmetric Key Cryptography (Secret Key Cryptography)
2.Asymmetric Key Cryptography (Public Key Cryptography)
3. Hash Function

1. Symmetric Key Cryptography (Secret Key Cryptography)
a) Same Key is utilized by the two gatherings
b) Simpler and Faster

2. Awry Key Cryptography (Public Key Cryptography)
a) Two diverse keys are utilized Users get the Key from a Certificate Authority.
b) Authentication in hilter kilter cryptography is more secured yet the procedure is generally more unpredictable as the declaration must be acquired from affirmation specialist

*3.2 Modern cryptography worries about the accompanying four goals:*
1) Confidentiality (the data can't be comprehended by anybody for whom it was unintended)
2) Integrity (the data can't be changed away or travel amongst sender and intende d recipient without the modification being distinguished)
3) Non-denial (the maker/sender of the data can't deny at a later stage his or her goals in the creation or transmission of the data)
4) Authentication (the sender and collector can affirm each other's character and the inception/goal of the data). There

  

are a few methods for ordering cryptographic algorithms. For motivations behind this paper, they will be sorted in view of the quantity of keys that are utilized for encryption and unscrambling, and additionally characterized by their application and utilize. Three sorts of algorithms that will be talked about here.

1. Symmetric Key Cryptography (Secret Key Cryptography)
2.Asymmetric Key Cryptography (Public Key Cryptography)
3. Hash Function

1. Symmetric Key Cryptography (Secret Key Cryptography)
a) Same Key is utilized by the two gatherings
b) Simpler and Faster

2. Awry Key Cryptography (Public Key Cryptography)
a) Two diverse keys are utilized Users get the Key from a Certificate Authority.
b) Authentication in hilter kilter cryptography is more secured yet the procedure is generally more unpredictable as the declaration must be acquired from affirmation specialist

*3.3 Modern cryptography worries about the accompanying four goals:*
1) Confidentiality (the data can't be comprehended by anybody for whom it was unintended)
2) Integrity (the data can't be changed away or travel amongst sender and intende d recipient without the modification being distinguished)
3) Non-denial (the maker/sender of the data can't deny at a later stage his or her goals in the creation or transmission of the data)
4) Authentication (the sender and collector can affirm each other's character and the inception/goal of the data).

## IV. CONCLUSION

In this Cryptography assumes essential part in dangerous development of computerized data stockpiling and correspondence. It is utilized to accomplish the mains of security objectives like secrecy, honesty, confirmation, non-revocation. Keeping in mind the end goal to accomplish these objectives, different cryptographic algorithms are produced. In which a portion of the algorithms are succeed and others bombed because of absence of security. The algorithm for encryption can be chosen in light of the sort of data being imparted and kind of channel through which data is being conveyed. The principle reason for this paper is to disperse the essential learning about the cryptographic algorithms and examination of accessible symmetric key encryption techniques in light of a few parameters like defenselessness to assault, Uniqueness about the method, and so on.

## REFERENCES

[1] Pawlan, M. (1998, February). Cryptography: the ancient art of secret messages. Retrieved May 4, 2009, from http://www.pawlan.com/Monica/crypto/.

[2] 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.

[3] Gary C. Kessler, An Overview of Cryptography, 1998-2015 — A much shorter, edited version of this paper appears in the 1999 Edition of Handbook on Local Area Networks, published by Auerbach in September 1998., http://www.garykessler.net/library/crypto.html.

[4] Vishwa gupta,2. Gajendra Singh ,3.Ravindra Gupta, Advance cryptography algorithm for improving data security, www.ijarcsse.com, Volume 2, Issue 1, January 2012 ISSN: 2277 128X.

[5] Siddharth Ghansela, Network Security: Attacks, Tools and Techniques, www.ijarcsse.com, Volume 3, Issue 6, June 2013 ISSN: 2277 128X.

[6] Image Encryption and Decryption using blowfish algorithm, World Journal of Science and Technology, Pg: 151-156.

[7] A Modified Approach for Symmetric Key Cryptography based on Blowfish Algorithm, Volume-1, Issue-6, and Pg: 79-82.

[8] A study of New Trends in Blowfish Algorithm, Volume-1, Issue-2, Pg: 321-326.

[9] Privacy and Authentication: An Introduction to Cryptography, proceeding of the IEEE, Volume-67, Number-3.

[10] Image Security using Encryption based Algorithm, International Conference on Trends in Electrical, Electronics and Power Engineering (ICTEEP), Pg: 110-112.

[11] Dhananjay M. Dumbere, Nitin j janwae "Video Encryption Using AES Algorithm" 2nd International Conference on Current Trends in Engineering and Technology, ICCTET'14 © IEEE 2014 IEEE Conference Number - 33344 July 8, 2014, Coimbatore, India.

[12] Ms. Pooja Deshmukh, Ms.vaishali khole "Modified AES Based Algorithm for MPEG Video Encryption" ICICES2014 - S. A. Engineering College, Chennai, Tamil Nadu, India. ISBN No. 978-1-4799-3834-6/14/$31.00 © 2014 IEEE

[13] S.Sridevi sathya Priya,P.Karthigai Kumar, N.M. SivaMangai, V.Rejula "FPGA Implementation of Efficient AES Encryption "IEEE Sponsored 2nd International Conference on Innovations in Information Embedded and Communication Systems ICIIECS'15 978-1-4799-6818-3/ 15/ $31.00 © 2015 IEEE

[14] JG pandey, S gurunarayan "Architectures and Algorithms for Image and Video Processing using FPGA-based Platform "978-1-4799-4006-6/14/$31.00 ©2014 IEEE

[15] Vakkayil Megha Gopinath "MAES Base Data Encryption and Description Using VHDL" © 2015 IJEDR | Volume 3, Issue 2 | ISSN: 2321-9939

[16] Cryptography The art of Hiding Information", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), ISSN: 2278 – 1323, Volume 2, Issue 12, December 2013.

  

[17] Irfan Landge et al., "Encryption and Decryption of Data Using Twofish Algorithm", World Journal of Science and Technology, ISSN: 2231-2587, Vol. 2, No. 3, pp. 157-161, 2012.

[18] Anjali Arora et al., "A Survey of Cryptanalytic Attacks on Lightweight Block Ciphers", International Journal of Computer Science and Information Technology & Security, ISSN: 2249-9555, Vol. 2, No. 2, April 2012.

[19] A. Grediaga et al., "Analysis and Implementation Hardware-Software of Rijindael Encryption", IEEE Latin America Transactions, Vol. 8, No. 1, pp. 82-87, March 2010.

[20] Ayushi, "A Symmetric Key Cryptographic Algorithm", International Journal of Computer Applications, ISSN: 0975 – 8887, Vol. 1, No. 15, 2010

  