International Journal of Recent Advancement In Engineering & Research

ISSN: 2456-401X Global Impact Factor: 0.864/1.0 Cosmos Impact Factor: 4.270/10

Symmetric Key Built Cryptographic Techniques

Sunil Satyadev,Prashant Gohel
Student,Saurastra University

Abstract:-. Information security has turned out to be most imperative angle for transmission of information and for capacity. Web is most normally and quick apparatuses for correspondence, sharing of data. Cell phones and electronic devices are much of the time utilized for sending and accepting of information utilizing web. In Symmetric key encryption just a single key is utilized to scramble and unscramble information. The key ought to be conveyed before transmission between two gatherings. Key assumes a critical part in encryption and unscrambling. On the off chance that a frail key is utilized as a part of the calculation then effectively information can be decoded. The measure of the key decides the quality of Symmetric key encryption. In the previous year a few calculation have been created for enhancing the effectiveness of Cryptographic calculations. Every last calculation utilized diverse methods and procedure to encryption and decoding the information. In this paper we speak to a relative investigation of different Symmetric key based encryptions, unscrambling calculations.
Keywords*:* Information, Cryptographic, encryptions,

I. INTRODUCTION

Cryptography is a procedure of scramble and decode messages or information in a manner that lone approved clients can read it. Imperative figures that involve cryptography are of some fundamental terms

1. Confidentiality:- This implies protection and Assurance of information
2. Authentication: - Data ought to be come to asserted client as it were.
3. Integrity: - This implies information ought not bothered by an unauthenticated individual.
4. Non-disavowal:- Means refusal insurance.
5. Access Control:- Prevents abuse of asset.
6. Availability: Data ought to be accessible with elite, non-deletion.

II. SECRET KEY CRYPTOGRAPHY

Mystery key cryptography methods utilized single key for both encryption and decoding.

Figure 1 indicate working procedure of Secret key cryptography strategies the sender utilizes the way to scramble the plaintext and sends the figure content to the collector. The beneficiary applies a similar key to decode the message and recoup the plaintext. Since a solitary key is utilized for both capacities, mystery key cryptography is additionally called symmetric encryption

III. LITERATURE REVIEW

In 2011 B. Ravi Kumar and Dr. P.R. K. Murti proposed" Data Encryption and Decryption handle Using Bit Shifting and Stuffing (BSS) Methodology". They proposed BSS technique I which they stuffing another piece in the place of unused piece which is moving from another printable character. So in BSS philosophy after encryption, for each eight bytes of plain content it will create seven bytes figure content and in decoding, for each seven bytes of figure content it will repeat eight bytes of plain content [5].

In 2012 Ch. Santhosh Reddy, Ch. Sowjanya and Shalini L proposed" Poly-alphabetic Symmetric Key Algorithm Using Randomized Prime Numbers. They give brief depiction about symmetric key calculations and proposed new calculation in symmetric key cryptography. The proposed calculation contains two levels of Exclusive OR (XOR) operation. The calculation is helpful in transmission of messages and information between one client and another [6].

In 2013 Obaida Mohammad Awad Al-Hazaimeh proposed "A New Approach for Complex Encrypting and Decrypting Data". They proposed A New Approach for Complex Encrypting and Decrypting Data" which keeps up the security on the correspondence channels by making it troublesome for assailant to predicate an example and speed of the encryption/decoding plan [2].

In 2013 Rachna Arora, Anshu Parashar proposed "Secure User Data in Cloud Computing Using Encryption Algorithms". They examined about distributed computing security issues, instrument, challenges that cloud specialist co-op confront amid cloud building and displayed the figurative investigation of different security calculations [3].

In 2013 Vineet Sukhraliya, Sumit Chaudhary, Sangeeta Solanki proposed "Encryption and Decryption Algorithm utilizing ASCII values with substitution cluster Approach". This calculation haphazardly created numbers are utilized with the assistance of modulus and leftover portion. Utilizing these modulus and leftover portion for getting another technique for encoding and unscrambling the message. The fundamental concentration is to furnish with an encryption unscrambling calculation with secure quality, conveying inability to the interloper push to break the cipher[12].

In 2014 C. J. Ulasi A. G. proposed "Investigation of Network Data Encryption and Decryption Techniques in Communication Systems". They display investigation of system information encryption and unscrambling strategies utilized as a part of correspondence frameworks. Fundamental reenactment program that encode and unscramble information were produced, composed and tried. Distinctive information piece sizes examination was made in light of the chart result[1].

In 2014 Satyajeet R. Shinge, Rahul Patil proposed" An Encryption Algorithm Based on ASCII Value". They show a symmetric cryptographic calculation for information encryption and decoding in view of ASCII estimations of characters in the plaintext. The calculation scrambles the plaintext utilizing their ASCII values. The mystery key is changed over to another string and that string is utilized as a key to scramble or decode the data[4].

III. ALGORITHMS EVALUATION PARAMETERS

(A) Structure and operation

Name of Algorithm	Structure and operation
TDES	The 3DES uses a 64 bit plain text with 48 rounds and a Key Length of 168-bits permuted into 16 sub- keys each of 48- bit length.
Blowfish	Blowfish is a block cipher that uses a 64 bit plain text with 16 rounds, allowing a variable key length.

Table 1. Structure and operation

(B) Scalability:-
It is one of the major element on which encryption algorithms can be analyzed. Scalability depends on certain parameters such as Memory Usage, Encryption rate, Software hardware performance and Computational efficiency.

(C) Strength

Name of Algorithm	Strength
Triple DES	DES operations (encrypt-decrypt-encrypt) are performed 3 times in 3DES with 2-3 different keys, offering 112 bits of security.
Blowfish	Blowfish's security lies in its variable key size (128-448 bits) providing high level of security.

Table 3. Strength of Algorithm

V. CONCLUSION

Cryptography assumes a vital part to secure information for correspondence and capacity. The fundamental objective of information security is privacy, honesty, validation, non-revocation. The fundamental reason for this paper is to spread the essential information about the cryptographic calculations and examination of accessible symmetric and deviated key encryption methods based Security, Flexibility and Architecture.

REFERENCES

I. C. J., Ulasi A. G "Analysis of Network Data Encryption & Decryption Techniques in Communication Systems" International Journal of Innovative Research in Science, Engineering and Technology (An ISO 3297: 2007 Certified Organization) Vol. 3, Issue 12, December 2014
II. Obaida Mohammad Awad Al-Hazaimeh A New Approach For Complex Encrypting And Decrypting Data International Journal of Computer Networks & Communications (IJCNC) Vol.5, No.2, March 2013
III. Rachna Arora and Anshu Parashar Secure User Data in Cloud Computing Using Encryption Algorithms International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 3, Issue 4, Jul-Aug 2013, pp.1922-1926
IV. Satyajeet R. Shinge , Rahul Patil An Encryption Algorithm Based on ASCII Value of Data Satyajeet R. Shinge (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (6) , 2014, 7232-7234
V. B. Ravi Kumar, Dr. P R. K. Murti Data Encryption and Decryption process Using Bit Shifting and Stuffing (BSS) Methodology B. Ravi Kumar et al. International Journal on Computer Science and Engineering (IJCSE) Vol. 3 No. 7 July 2011
VI. Ch. Santhosh Reddy, Ch. Sowjanya, P. Praveena, Shalini L Poly-alphabetic Symmetric Key Algorithm Using Randomized Prime Numbers International Journal of Scientific and Research Publications, Volume 2, Issue 9, September 2012 1 ISSN 2250-3153
VII. Sombir Singh and Sunil K. Maakar Enhancing the Security of DES Algorithm Using Transposition Cryptography Techniques " International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 6, June 2013