ANALYSIS OF SYMMETRIC KEY CRYPTOGRAPHIC ALGORITHMS

SurekhaThorat[1] Rohini Sharma [2] Shivaji Pansare[3]

Abstract: *Today information has become the most powerful commodity & communication online or through wireless network .Also there are number of financial and personal data application developed but real need of security because there are various passive and active attacks. We use typical security mechanism like password security or encoding data .Cryptography is best solution for security .Cryptography means encoding message in non readable format it is called encryption and convert message in to non readable to readable format called decryption .This paper represent analysis of various symmetric key cryptographic algorithms .*

Keywords : Symmetric key algorithm ,DES DOUBLEDES,IDEA,AES,RC4,RC5,RC6, Blowfish

1.INTRODUCTION

Today transaction and Exchanging data using internet is become very efficient part of day to day life. Variety of Confidential data is exceeded through internet which include defense record, password, bank related data, medical records personal information etc. These information should always be protected from hackers .There are various encryption algorithm are used for data protection .Cryptography algorithm play important role in data protection .In cryptography message hidden from unauthorized user and only Authorized recipient will able to convert it into original message. There are Symmetric Encryption algorithms and asymmetric algorithm both are play important role in information security. If encryption algorithm take long time for execution then it is useless. Today more and more sensitive data is being stored on computers and transmitted over the Internet. So we need security and safety of information. In this paper We discuss about different Symmetric key Cryptography Algorithm.

2. SYMMETRIC KEY CRYPTOGRAPHY ALGORITHM

Here same secrete key is used for encryption and decryption .but big problem here key distribution /key exchange using same key .Sender and receiver use same secrete key which is hidden and this key is use for encryption and decryption but both the parties must agree upon the key before any transaction begins and nobody else should know about it .If anyone get this key easily obtained hidden message. Plain text message, secrete key, cipher text message and Symmetric algorithm for encryption and decryption play important role in cryptography model.

2.1 Overview of Some Common Symmetric Algorithm

There are two types of encryption algorithms stream ciphers provide bit by bit and block cipher provide block by block encryption.

A. Data Encryption Standard (DES) It is generally used in ECB,CBC,CFB mode. It was designed by IBM based on their Lucifer Cipher[10]. The origin of DES go back to 1972 by National Institute of Standards and Technology (NIST) and embarked a DES encrypt data in block of size 64 bits each .It has input 64 bits of plain text and produce 64 bits cipher text output.Before DES process start every eight bit of the key is discarded to produce 56-bit key .It use substitution and transposition .[9]It contain 16 round .First it perform initial permutation function(IP).IP happens only once before round start .IP produce two halves LPT and RPT .Each half block consist of 32bits.Then start round first operation is key transformation which generate 48 bit sub key from 56 bits. Then Expansion permutation perform on RPT is expanded from 32 bits to 48 bits .Then 48 bit key is XORed with 48 bit RPT and then resulting output is given to S-box substitution .It accept 48 bit input and expand RPT and produce 32 bit output. Last stage is p-box permutation. Output of 32 bits is permuted using P-box. All these steps perform on 32 bit RPT .Here LPT are untouched so at these stage LPT XORed with output produced by p-box permutation. Then get new right half .At the end of 16 rounds Final permutation is performed by using simple transposition techniques. It had been also observed that decryption of DES algorithm is better than other symmetric algorithms in throughput and less power consumption[1]

B.Double DES It perform twice what DES normally does once . It use 64 bit plain text block and 56 bit key. So we will need to store 2^{56} 64 bit block to store the table in memory. There are chances of Meet in the middle attack.

C.International Data Encryption Algorithm (IDEA) It was launched in1990.It required licensed before it can use in application .Also it has tracking record .IDEA is block cipher.It has input as 64 bit plain text block and use 128 bit longer key .Input divided into four portion .Then perform eight rounds .Last step is output transformation .IDEA use 128 bit key which is double than DES So it required 2^{128} operation and which is very difficult to break IDEA [10]. Today, in many market areas,

ranging from Financial Services, and Broadcasting to Government available IDEA based security .Typical fields are where IDEA used in embedded in audio and video data for cable TV, pay TV, video conferencing, distance learning, business TV, Sensitive financial and commercial data, Email via public networks Also transmission links via modem, router or ATM link, GSM technology also Smart cards.

D.Advanced Encryption standard (AES) AES used in Smart cards and smart phones because it work very fast.It use large block size(128 bit) and longer keys therefore it is more secure . According to NIST AES is replacement for 3DES Even though AES has theoretical advantage over 3DES for speed and efficiency .[4]

E.RC4 Also known as ARC4 . Officially it is called "Rivest Cipher 4" designed by Ron Rivest in 1987. It is stream cipher . Widely used in encryption standard including Wireless Equivalent Private (WEP) for wireless card and TLS. [10]RC4 is used stream cipher. RC4 is good if the key is never reused. The cipher can be expected to run very quickly insoftware. It was considered secure until it was vulnerable to the BEAST attack.[11]

F. RC5 Algorithm develop by Ron Rivest .It is fast and used for primitive operation .It allows variable number of rounds and variable key size .It requires less memory for execution so it is suitable for smart card and other devices .It has been incorporated into RSA Data security Incorporation's product such as BSAFE ,JSAFE. .RC5 has three important parameter word size in bits, number of rounds, number of 8 bit bytes in key .It perform number of step and rounds to get security .RC5 required low memory. It use magic numbers. It is suitable for hardware or software. Due to the data-dependent rotations, differential cryptanalysis and linear cryptanalysis is not possible. The key used is strong if it is long. However, if the key size is short, then the algorithm is weak.

G.RC6 It was developed in 1997. It is a block cipher which uses 128 bit block size and supports key sizes of 128, 192 and 256 bits. [11]RC6 also provide requirements of the AES. It is an improvement of the RC5 Algorithm. It provides even better securityRC6 does use an extra multiplication operation not present in RC5 in order to make the rotation dependent on every bit in a word, and not just the least significant few bits. [10]

H. Blowfish Blowfish is 64 bit fastest block cipher algorithm and used to replace DES or IDEA. It was developed by Bruce schneier in 1993. It is accomplish objectives as compact, fast ,simple and secure . Ranging from 32 bits to 448 bits, variable length key is used. Variants of 14 round or less are available in Blowfish. Blowfish is unpatented and license-free and is available free for all uses[10]. Blowfish suffers from weak keys problem.

I.RSA It depend on factor n into p and q . Rivest, Shamir, and Adleman suggested using 100-digit numbers for p and q then n is 200 digits, and factoring would take several billion years at the rate of one step per microsecond.[11] .RSA use Public-key encryption and Digital signatures. The receiver may need to verify that a transmitted message actually originated from the sender and didn't just come from there authentication.RSA use for electronic transaction.There have been numerous attacks proposed against RSA.There are made some proposals to build special computers whose sole purpose is to break RSA. Proposals include an optoelectronic factoring machine and several other architectures based on conventional semiconductor technology.

3.CONCLUSION

This paper attempts to review major researches and developments occurred in Symmetric key cryptography .We analyses many Symmetric algorithm and there steps. Symmetric key cryptography understood as the technique which uses a single key for the encryption as well as the decryption of data. This paper provides an overview of Symmetric algorithm are implemented in the recent scenario which provide efficiency and effectiveness. Today research start on role of symmetric algorithm in DNA cryptography, quantum cryptography.

4.REFERENCE

[1] Mohit Marwaha, Rajeev Bedi,Amritpal Singh, Tejinder Singh, Comparative Analysis Of Cryptographic Algorithms Singh et al., International Journal of Advanced Engineering Technology e- ISSN 0976- 3945

[2] Preeti Singh , Praveen Shende Symmetric Key Cryptography: Current Trends IJCSMC, Vol. 3, Issue. 12, December 2014

[3] VikasAgrawal ,Shruti Agrawal , Rajesh Deshmukh Analysis and Review of Encryption and Decryption for Secure Communication ,ISSN (Online): 2347-3878 Volume 2 Issue 2, February 2014

[4] Md. Sarfaraz Iqbal Shivendra Singh ArunimaJaiswal, Symmetric Key Cryptography: Technological Developments in the Field, Volume 117 – No. 15, May 2015

[5] Saranya K,Mohanapriya R ,A Review on Symmetric Key Encryption Techniques in Cryptography, International Journal of Science, Engineering and Technology Research (IJSETR), Volume 3, Issue 3, March 2014

[6] JyotirmoyDas ,A Study on Modern Cryptography and their Security Issues,

ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 4, Issue 10, October 2014)
[7] Rejani. R ,Deepu.V. Krishnan 2,Study of Symmetric key Cryptography Algorithms, International Journal of Computer Techniques -– Volume 2 Issue 2, Mar - Apr 2015
[8] NiveditaBisht ,Sapna Singh , A Comparative Study of Some Symmetric and Asymmetric Key Cryptography Algorithms ,Vol. 4, Issue 3, March 2015
[9] PrekshaNemaM.A.Rizvi,Critical Analysis of Various Symmetric Key Cryptographic Algorithms Volume: 3 Issue:6
[10] Atul Kahate ,*Cryptography and Network security* (Tata Mc-Graw Hill publishing company limited 2008)
[11] Milind Mathur ,Ayush Kesarwani, Comparison Between DES,3DES , Rc2 , Rc6 , Blowfish and AES, Proceedings Of National Conference On New Horizons In It - NCNHIT 2013
[12] Sheetal Charbathia and Sandeep Sharma "A Comparative Study of Rivest Cipher Algorithms" ISSN 0974-2239 Volume 4, Number 17 (2014)