Symmetric Key Generation Algorithm Using Sum Of Subset N-P Problem.

Haseeb Ahmed
Computer Science & Engineering
G.C.E.T.
Greater Noida, India
haseebahmed4884@gmail.com

Abstract: ***Information security is the process of protecting information. It protects its availability, privacy and integrity. Access to stored information on computer databases has increased greatly. More companies store business and individual information on computer than ever before. Much of the information stored is highly confidential and not for public viewing. Here presenting a new "Symmetric Key" Generation algorithm. This algorithm is using "Sum of subset N-P problem" results in a Symmetric Key with increased strength While keeping the key size optimized which taking constant time to run.***

Index Terms:

Encryption,Algorithm,Complexity,Symmetric,Asymmetric , NPcomplete,X-OR,Blowfish,AES,DES.

Introduction:

Cryptography is usually referred to as "the study of secret". Encryption is the process of converting normal text of unreadable form.Decryption is the process of converting encrypted text to normal text in the readable form.

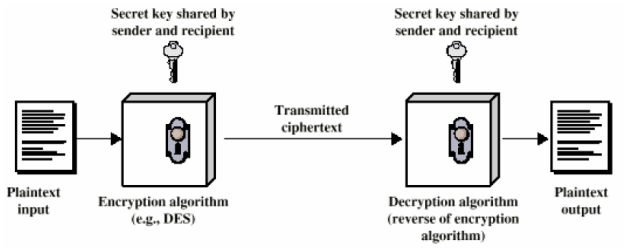

Fig. 1. A Simplified Model of Conventional Cryptography

CIPHERTEXT

It means that only the authenticated people are able to interpret the message content and no one else.

INTEGRITY

Assuring the receiver that the received message has not been altered in any way from the original.

NON-REPUDIATION

A mechanism to prove that the sender really sent this message. Means that neither the sender nor the receiver can falsely deny that they have sent a certain message.

SERVICE RELIABILITY AND AVAILABILITY

Since secure systems usually get attacked by intruders,which may affect their availability and type of service to their users Such systems provide a way to grant their user the quality of service they expect.

SYMMETRIC AND ASYMMETRIC ENCRYPTIONS

Asymmetric Encryption is also called as public key cryptography. It uses two keys: public key,which is known to public using in encryption and private key, which is known only to the user of that key using in decryption .The public and the private keys are related to each other by any mathematical means.In other words data encrypted by one public key can be encrypted only by its corresponding private key.

Symmetric key Encryption is also called as single key cryptography. It uses a single key. In this encryption process the receiver and the sender has to agree upon single secret key

ISBN: 9788175157538

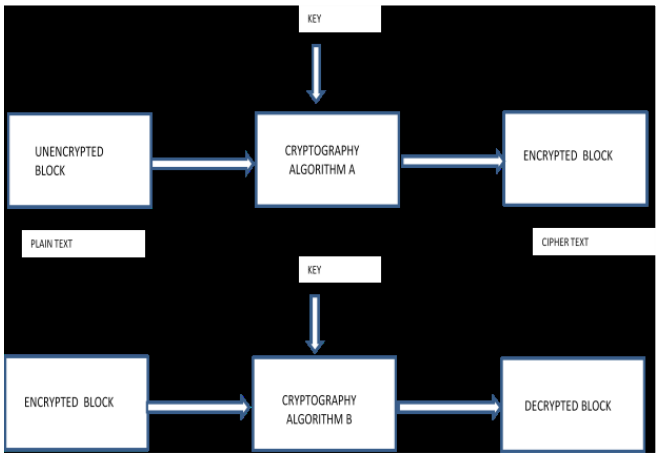

Fig. 2. Basic Concept of Symmetric Cryptography.

Proposed Work:

Here presenting a symmetric key generation algorithm produses symmetric key using in block based symmetric cryptography. This algorithm is based on the concept of " sum of subset " N-P complete problem ". Here algorithm taking constant time to generate key such that the strength of key is better than exiting symmetric key algorithm while keeping the key size optimum.

Steps of proposed Algorithm:

1- Create a 2048(256*8) bits number.

2-Divide above number into 4 numbers(n1,n2,n3,n4 each of size2048 bits) such that the sum of these numbers is equal to above number.

3-Divide n1 into 8 blocks(n11,n12,n13,n14,n15,n16,n17,n18) each of size 256 bits.

4-Perform XOR Operation on(n11,n12),(n13,n14),(n15,n16)

(n17,18)and named as (n1112, n1314, n1516, n1718) correspondingly .

5-Perform XOR Operation on (n1112,n1314),(n1516,n1718) and named as n11121314, n15161718 correspondingly and again Perform X-OR Operation on (n11121314, n15161718) named as n11121314 , 15161718 (256 bits) again named as Na.

6- Repeat Steps 3, 4, 5 for All n2 ,n3,n4 Results Values as Nb,Nc,Nd.

7-Now Apply X-OR Operation on (Na ,Nb) , (Nc ,Nd) and named as Nab , Ncd correspondingly .

8-Finally Apply X-OR Operation on (Nab,Ncd) and Named as Nabcd(Final Key) .

9-Exit.

Explaination Of Proposed Alorithm:

Here in the first step the sender select a 2048 (256*8) bit random binary number ,So this selected number is one of the all 2^2048 numbers.

In the second step using the concept of sum of subset n-p problem. The above 2048 bit binary number is divided into four parts , each of 2048 bits such that the sum of all these four numbers is equal to randomly selected above 2048 bit number.

These four numbers are not fixed numbers,but the constaints with these numbers are-

a) Each of the four numbers should be of size 2048 bit.

b) The sum these four numbers should be equal to initially selected 2048 bit number.

Finally these selected four numbers are named as N1, N2,N3 and N4,Respectively.

In third step of the algorithm the number N1 is divided into four parts each of size 256 bits. And each number is named as N11, N12, N13, N14, N15, N16, N17, and N18 respectively.

In the fourth step, X-OR operation is performed in between numbers of each pair(N11,N12),(N13,N14),(N15,N16),(N17 ,N18) and the resulted sum of each pair is named as N1112 , N1314 , N1516 , N1718 respectively.

Now , again X-OR operation is performed in-between the numbers of each pair (N1112, N1314), (N1516, N1718). and the resulted sum of each pair is named asN11121314,N1516 1718 respectively

Again the numbers N11121314 and N15161718 are undergo X-OR operation and the final resulted sum is named as "Na" This final number Na is of size "256" bits.

Each number N2,N3,N4 undergoes all the above 2, 3, 4 , and 5 steps resulting in numbers each of size 256 bits named as Nb, Nc, Nd respectively.

Numbers (Na, Nb) and (Nc, Nd) undergoes X-OR operation and the resulted sum named as Nab, Ncd.

Finally,the number Nab and Ncd undergoes X-OR operation and produces the final key as Nabcd (FINAL KEY).

ISBN: 9788175157538

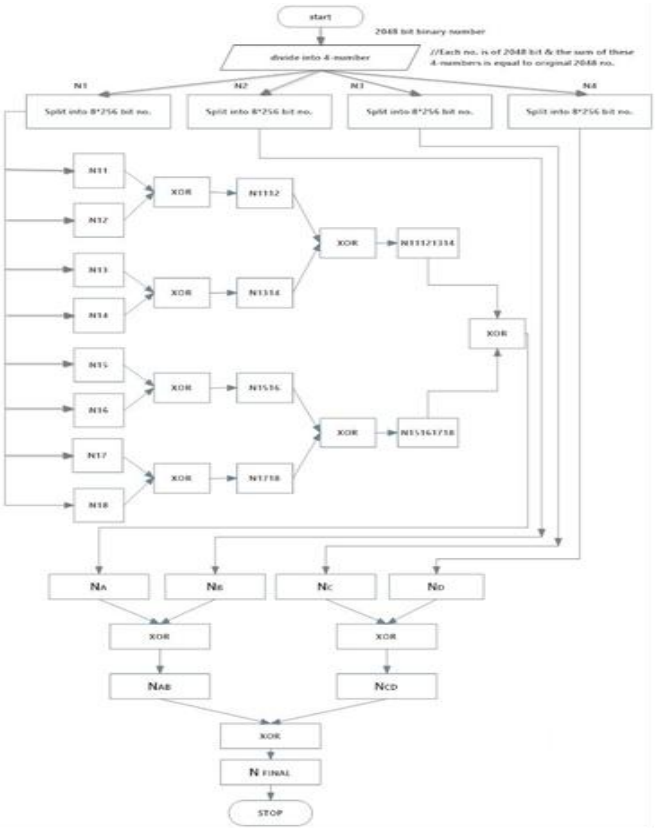

Fig. 3. Flow Chart Representing steps of above Algorithm.

Results And Comparision:

Table. 1. Comparision Of Stength,key Size and Encryption time of different Techniques.

Technique	**Strength (Complexity)**	**Key size(bits)**	**Encryption Time**
DES	***2^39-2^43***	***56***	***16 rounds***
AES	***2^254.4***	***128-256***	***14 rounds***
BLOWFISH	***2^128***	***32-448***	***16 rounds***
3-DES	***2^N(N is size of key)***	***56-168***	***48 des rounds***
PROPOSED	***2^2048***	***256***	***Constant time***

Conclusion and Future Enhancement

The Proposed work aims to increase the strength of the key while keeping the size of the key optimized ,So that the encpted data is more difficult to crack by a bruteforce technique since the key size is optimized ,so the overhead of data encryption is also not increased.

Conclusion is, the strength of encrypted data is increasing as compared to exiting symmetric encryption algorithm while keeping the encryption overhead optimized.

Algorithm can be used for Symmetric Encryption of Data while maintaining the Integrity and Sucurity of the Confidential data.

References

[1] Dripto Chatterjee , Joyshree Nath , Suvadeep Dasgupta, Asoke Nath"A new Symmetric key Cryptography Algorithm using extended MSA method : DJSA symmetric key algorihm published in 2011 International Conference on Commun -ication Systems and Network Technologies , 978-0-7695-4437-3/11 $26.00 © 2011 IEEE.

[2] Yan Wang and Ming Hu " Timing evaluation of the known cryptographic algorithms " 2009 International Conference on Computational Intelligence and Security 978-0-7695-3931-7/09 $26.00 © 2009 IEEE DOI 10.1109/CIS.2-009.81.

[3] Symmetric key cryptography using random key generator, A.Nath, S.Ghosh, M.A.Mallik, Proceedings of International conference on SAM-2010 held at Las Vegas(USA)12-15 July,2010, Vol-2,P-239-244.

[4] Data Hiding and Retrieval,A.Nath,S.Das,A. Chakrabarti, Proceedings of IEEE International conference on Computer Intelligence and Computer Network held at Bhopal from 26-28 Nov, 2010.

[5] Neal Koblitz "A Course in Number Theory and Cryptography" Second Edition Publishedby SpringerVerlag.

[6] By Klaus Felten"An Algorithm for Symmetric Cryptography with a wide range of scalability " published by 2nd International Workshop on Embedded Systems, Internet Programming and Industial IT.

[7] Majdi Al-qdah & Lin Yi Hui "SimpleEncryption/ Decryption Application " published in International Journal of Computer Science and Security, Volume (1) : Issue (1).

[8] T Morkel, JHP Eloff " ENCRYPTION TECHNIQUES: A TIMELINE APPROACH" published in Information and Computer Security Architecture (ICSA) Research Group proceeding.

[9] Text book William Stallings , Data and Computer Communications, 6eWilliam 6e 2005.

[10] Md. Nazrul Islam, Md. Monir Hossain Mia Muhammad F. I. Chowdhury, M.A. Matin "Effect of Security Increment to Symmetric Data Encryption through AES Methodology" Ninth ACIS International Conference on Software Engineering , Artificial Intelligence , Networking , and Parallel / Distributed Computing 978-0-7695-3263-9/08 DOI10.1109/ SNPD.2008.101 IEEE 2008.

ISBN: 9788175157538

[11] [Rijn99] Joan Daemen and Vincent Rijmen , AES submission document on Rijndael,Version 2,September1999

[12] Design and Analysis of Algorithm by coreman.

[13]http://en.wikipedia.org/wiki/Data_Encryption_Standard

[14]http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

[15]http://en.wikipedia.org/wiki/Blowfish_(cipher)

[16] Volume 2 , Issue 1 , January 2012 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering

[17]http://www.ece.ucsb.edu/~parhami/rsrch_paper_gdlns.htm

[18] International Journal of Emerging Technology and Advanced Engineering

Website: www.ijetae.com (ISSN 2250-2459,Volume 1,Issue 1, November 2011)

[19] Zobel, J., Writing for Computer Science, Springer, 2nd ed., 2004. [T11.Z62 2004]

[20] http://en.wikipedia.org/wiki/Cryptography

ISBN: 9788175157538