International Journal of Scientific Engineering and Technology (ISSN : 2277-1581)
Volume No.3 Issue No.8, pp : 1123-1125 1 Aug 2014

Symmetric and Asymmetric Cryptography Algorithm for Improving Data Security

Jasdeep Dhillon
University College of Engineering Punjabi University Patiala
Dhillon_0051@yahoo.co.uk

***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 stores business and individual information on computer than ever before. Mush of the information stored is highly confidential and not for public viewing. In this paper I have developed a new cryptography algorithm which is based on block cipher concept. In this algorithm I have used logical operation like XOR and shifting operation. Experimental results show that proposed algorithm is very efficient and secured.*

***Keywords:** Information security, Encryption, Decryption, Cryptography*

Section – I : Introduction

The main feature of the encryption/decryption program implementation is the generation of the encryption key. Now a day, cryptography has many commercial applications. If we are protecting confidential information then cryptography is provide high level of privacy of individuals and groups. However, the main purpose of the cryptography is used not only to provide confidentiality, but also to provide solutions for other problems like: data integrity, authentication, non-repudiation. Cryptography is the methods that allow information to be sent in a secure from in such a way that the only receiver able to retrieve this information. Presently continuous researches on the new cryptographic algorithms are going on. However, it is a very difficult to find out the specific algorithm, because we have already known that they must consider many factors like: security, the features of algorithm, the time complexity and space complexity. Figure 1 is representing conventional encryption

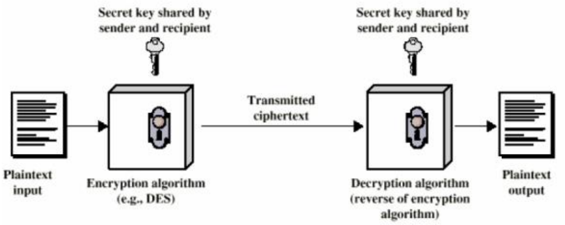

Secret key shared by sender and recipient
Secret key shared by sender and recipient
Transmitted ciphertext
Plaintext input
Encryption algorithm (e.g., DES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

Figure 1: A Simplified Model of Conventional Encryption

Security Services: If we are taking about security of information then following services come in mind.

□ Confidentiality (privacy)
□ Authentication (who created or sent the data)
□ Integrity (has not been altered)
□ Non-repudiation (the order is final)
□ Access control (prevent misuse of resources)
□ Availability (permanence, non-erasure)

Section – II

Here a newly developed technique named, “A new Symmetric key Cryptography Algorithm using extended MSA method: DJSA symmetric key algorithm” [1] is discussed. In this they are suggesting a symmetric key method where they have used a random key generator for generating the initial key and that key is used for encrypting the given source file. In this method basically a substitution method where they take 4 characters from any input file and then search the corresponding characters in the random key matrix file after getting the encrypted message they store the encrypted data in another file. For searching characters from the random key matrix they have used a method which was proposed by Nath in MSA algorithm. In that they have the provision for encrypting message multiple times. The key matrix contains all possible words comprising of2 characters each generated from all characters whose ASCII code is from 0 to 255 in a random order. The pattern of the key matrix will depend on text key entered by the user. They are proposing their own algorithm to obtain randomization number and encryption number from the initial text key entered by the user. They are proposing their own algorithm to obtain randomization number and encryption number from the initial text key. they have given a long trial run on text key and they have found that it is very difficult to match the above two parameters from 2 different Text key which means if someone wants to break his encryption method then he/she has to know the exact pattern of the text key. To decrypt any file one has to know exactly what is the key matrix and to find the random matrix theoretically one has to apply 65536! trial run and which is intractable. They have apply method on possible files such as executable file, Microsoft word file, excel file, access database, FoxPro file, text file, image file, pdf file, video file, audio file, oracle database and they have found in all cases it giving 100% correct solution while encrypting a file and decrypting a file. This method can be used for encrypting digital signature, watermark before embedding in some cover file to make the entire system full secured. In the following section we are going in detail. Here another newly developed technique named, “Effect of Security Increment to Symmetric Data Encryption through AES Methodology” [09] is discussed. In this method they describe about symmetric cipher algorithm which is much more similar to Rijndael. The difference is that, Rijndael algorithm start with 128 bits block size, and then increase the block size by appending columns[10], whereas his algorithm start with 200 bits.

Proposed Work:

Combining Symmetric And Asymmetric Algorithms

Since there is no secret key exchange required in order to use asymmetric algorithms, you might be tempted to solve the symmetric key exchange problem by simply replacing the symmetric algorithm with an asymmetric algorithm. We still want to take advantage of the superior speed and security offered by symmetric algorithms, so instead, we actually combine the two (and sometimes more than two) algorithms.

For example, Microsoft Outlook and Netscape Communicator implement secure email using the S/MIME (Secure/Multipurpose Internet Mail Extensions) specification. S/MIME is an IETF standard that supports both digital signatures for authentication and encryption for privacy. S/MIME provides bulk message data encryption using any of several symmetric algorithms, including DES, 3DES, and RC2.

As another example, the popular PGP software provides cryptographic services for email and file storage by combining several algorithms to implement useful cryptographic protocols. In this way, message encryption and digital signatures are provided to email clients using an assortment of selected symmetric, asymmetric, and hash algorithms. RSA or ElGamal are used for PGP session key transport. 3DES is one of several alternatives used for bulk PGP message encryption. PGP digital signatures use either RSA or DSA for signing and MD5 or SHA 1 for generating message digests.

There are several other protocols that are built in a hybrid manner by combining asymmetric and symmetric algorithms, including IPSec and SSL IPSec is an IETF standard that provides authentication, integrity, and privacy services at the datagram layer, allowing the construction of virtual private networks (VPNs). The SSL protocol, developed by Netscape, provides authentication and privacy over the Internet, especially for HTTP (Hypertext Transfer Protocol).

So from the previous chapters discussions i came to point and suggested the proposed asymmetric algorithm which takes the idea from symmetric algorithm and is implemented in asymmetric algorithm which will increase the security level in the data transmission communication

Generally RSA and DES both are encryption mechanism. But RSA produces the single key encryption and single key decryption. Single key encryption and decryption has high rate of predictability. So i enhance this algorithm by attaching DES to it, such that security level can be increased. Each involves 10 rounds encryption and decryption which provides the extra encryption to the algorithm. Even if the encryption and decryption keys are known to others but the 10 round mechanism cannot be known and one cannot decrypt the message unless user knows the 10 rounds.If we combine the two cryptographic mechanism, so to achieve the better of two, and till extent some of the following requirements can met Complete secure solution

- Time taken by the encryption and decryption process is less
- Generated cipher is of compact size
- Key distribution problem is solved

Proposed Asymmetric Algorithm

This algorithm is based on fundamental attributes of cryptography: substitution and transposition. It consists of 10 steps, each of which is called a round. Each round performs the steps of substitution and transposition.

- Choose two large numbers P and Q.

Calculate N = P*Q.

- Select the public key (encryption key) E, such that it is not a factor of (P-1) and (Q-1).
- For Encryption, calculate the cipher text (CT) as follows

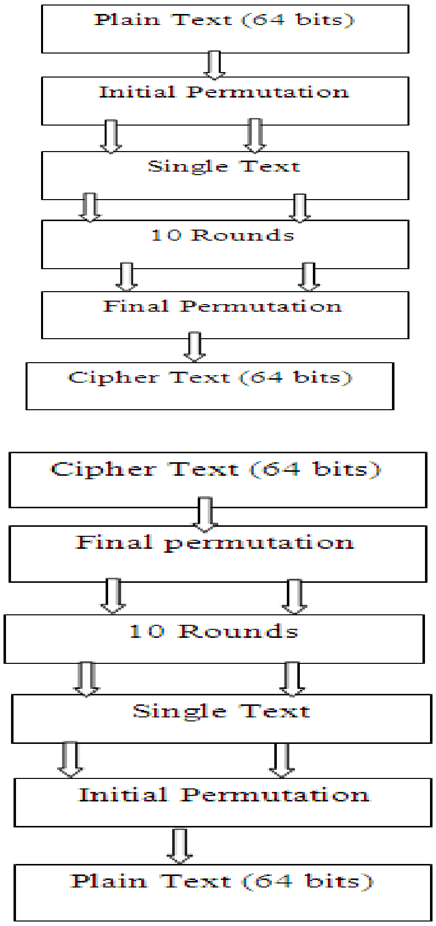
$CT = PT^{E} \bmod N.$

- Send CT as cipher text to the receiver
- Select the private key (decryption key) D such that the following equation is true

$D*E \bmod (P-1)*(Q-1) = 1.$

- For Decryption, calculate the plain text (PT) form the cipher text as follows

$PT = CT^{D} \bmod N$



RSA Performance Analysis of Encryption Algorithms

Encryption key size 22 bits

Decryption key size 10 bits

Text Size	Encryption	Decryption
128 Bits	0.0549	0.0549
256 Bits	0.1098	0.0549
512 Bits	0.2197	0.1648
1K	0.3846	0.3296
2K	0.7142	0.6593
5K	1.7032	1.7032
10K	3.402	3.402

TABLE 1 RSA Encryption And Decryption Methods Computational Execution Timing Seconds

Key Size 56 Bits

Text Size	Encryption	Decryption
128 Bits	0.054945	0.00001
256 Bits	0.054946	0.00001
512 Bits	0.070976	0.00052
1K	0.1418	0.0010
2K	0.2835	0.0020
5K	0.6816	0.0084
10K	1.3601	0.0142

TABLE DES Encryption And Decryption Methods Computational Execution Timings In Seconds

Text Size	Encryption	Decryption
128 Bits	0.109845	0.05491
256 Bits	0.1664746	0.05491
512 Bits	0.290676	0.16532
1K	0.5264	0.3306
2K	0.9977	0.6613
5K	2.3848	1.7404
10K	4.7621	3.4162

TABLE proposed algorithm Encryption And Decryption Methods Computational Execution Timings In Seconds

Method	Des	Rsa	Proposed Hybrid
Complexity	O(Log N)	O(N^{3})	O(Log N +N^{3})
Security	Moderate	High	Highest

CONCLUSION

As the performance of des in decryption process is quiet high than other techniques. Despite the key distribution des is more suitable to the applications which has the decryption as the highest priority, but when we talk about security there is no doubt than asymmetric key cryptography system provides more security. But by combining both the algorithms we can cover the disadvantages of both symmetric and asymmetric key cryptography to some extent.

REFERENCES

i. Atul kahate, " Cryptography and Network Security", Second edition, Tata Mcgraw Hill, 2008, page

ii. Rolf Oppliger, "Contemporary Cryptography", Library of Congress Cataloging inPublication Data,page 1-3

iii. Joe Harris, "Cisco Network Security Little Black Book" ,The Coriolis Group LLC Texas, 2002, page 156-165

iv. Serge Vaudenay, "A Classical Introduction To Modern Cryptography Applications For Communications Security", Springer Science+Business Media,2006

v. J. Lopez and J. Zhou, "Wireless Sensor Network Security", IOS Press, 2008, Page 45-46

vi. A. Menezes, P. van Oorschot and S. Vanstone",Handbook of Applied Cryptography" CRC Press,1997,page. 4

vii. William stallings, "Data And Computer Communication 5 Th Edition Reprinted", Prentice Hall, 2003, page 624-634

viii. William Stallings , "Cryptography and Network Security Principles and Practices, Fourth Edition", Prentice Hall, 2005, Page 13 -15

ix. Roger Dube, "Hardware-Based Computer Security Techniques to Defeat Hackers", John Wiley & Sons, Inc., 2008, Page 18-37

x. Dr. Eric Cole, Dr. Ronald Krutz, and James W. Conley, "Network Security Bible", Wiley, 2005, Page 462-465

xi. C. Paar, J. Pelzl, "Understanding Cryptography", Springer ,2010, Page 29-

xii. J.M. Kizza, "A Guide to Computer Network Security", Springer, 2009, Pg 230-236

xiii. Mark Ciampa, "SECURITY+ 2008 IN DEPTH", Course Technology, a part of Cengage Learning Boston, 2009, Page 295-296

xiv. Julius Caesar, "Codes and ciphers", Published by the press syndicate of the university of Cambridge, page 183-188, 2004

xv. J. Lopez and J. Zhou , "Wireless Sensor Network Security" ,IOS Press, 2008, Pg 293 -298

xvi. Jan Pelzl, "Understanding Cryptography" Springer,2010, Pg 87-91

xvii. Jie Wang, "Computer Network Security Theory and Practice", Springer, 2009 Pg 57

xviii. Tom St Denis, "Cryptography for Developers", Syngress Publishing, Inc, 2007, Pg 140-142

xix. Sheikh Muhammad Farhan, ShoabA.Khan, Habibullah Jamal ,Microprocessors and Microsystems 33 journal "An 8-bit systolic AES architecture for moderate data rate applications" ,2009, pg 222-224

xx. Eric Knipp, Brian Browne, Woody Weaver, C. Tate Baumrucker, Larry Chaffin, Jamie Caesar, Vitaly Osipov, "Managing Cisco Network Security", Second Edition, Syngress Publishing, Inc,2002, Page 480

xxi. Lydia Parziale, David T. Britt, Chuck Davis, Jason Forrester, Wei Liu, Carolyn Matthews, Nicolas Rosselot, "TCP/IP Tutorial and Technical Overview", International Business Machines Corporation 1989-2006, Eighth Edition (December 2006), Pg 784

xxii. David Bishop, "Introduction To Cryptography With Java Applets", Jones and Bartlett Publishers, Inc.,2003 Page 259-260