DATA SECURITY USING COMPREHENSIVE RSA CRYPTOGRAPHIC ALGORITHM

G.Amala[1], A.Komathi[2]

[1]Research Scholar, Department of Computer Science & Information Technology,
Nadar Saraswathi College of Arts & Science, Theni, Tamil Nadu, (India)
[2]Department of Computer Science & Information Technology,
Nadar Saraswathi College of Arts & Science, Theni, Tamil Nadu, (India)

ABSTRACT

Data Security is the method of shielding information. More companies store business and individual information on computer than ever before. In the existing research, cryptographic block cipher concept with logical operation like XOR and shifting operation were used. In this the main drawback was that, generate key was based on Alphabets only. So any hackers had the chance to find out the secret random key using loop concept.

So In my Research, I proposed RSA cryptographic algorithm which uses Key Generation Algorithm with Hashing Function technique to encrypt and decrypt the given data. The Key will be generating by using Key Generation Algorithm and the Key will be based on higher sets of alphanumeric characters. So the Crypt analyzing process will be difficult compare to the previous one. Moreover, Here I used Hashing Technique for Cryptographic along with Qubit Key Generation Method. Experimental result will show the efficiency and security of my proposed algorithm.

Key Words: Information Security, Block Cipher Method, RSA Algorithm, Hashing Technique, Key Generation Method

I. INTRODUCTION

Information security has become a very critical aspect of modern computing system. With the global acceptance of the Internet, virtually every computer in the world today is connected to every other. While this has created incredible productivity and unprecedented opportunities in the world we live in, it has also created new risk for the user of these computers. The user, businesses and organisations worldwide have to live with a constant threat from hackers and attackers, who use a variety of methods and tools in order to break into computer system, steal information, change data.

Now a day, cryptography has many commercial applications. If we are shielding confidential data then cryptography is provide high level of privacy of individuals and groups. However, the main scope of the cryptography is used not only to provide confidentiality, but also to provide solution for other problems like: data integrity, non-repudiation, and authentication.

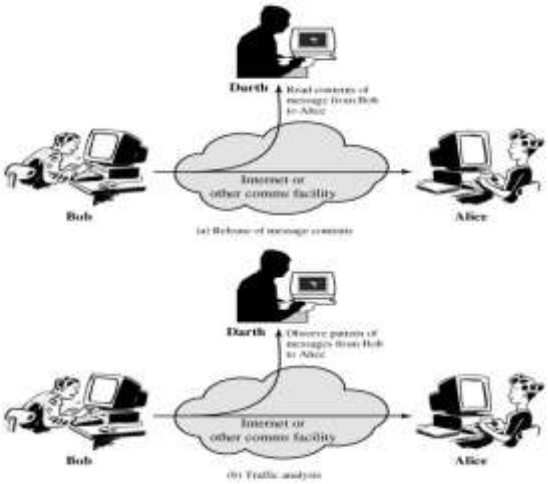

Darth
Read contents of message from Bob to Alice
Internet or other comms facility
Bob
Alice
(a) Release of message contents
Darth
Observe pattern of messages from Bob to Alice
Internet or other comms facility
Bob
Alice
(b) Traffic analysis

Fig 1 Passive Attacks

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 very complicated to find out the specific algorithm, because we have previously known that they must consider many factors like: security, the features of algorithm, the time complexity and space complexity.

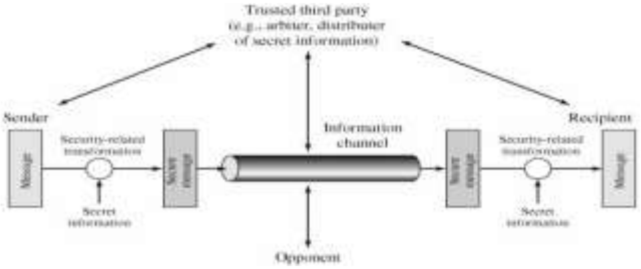


Fig 2 Model for Network Security

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 misuses of resources)
- Availability (permanence, non-erasure)

II. LITERATURE REVIEW

2.1 Advance Cryptography Algorithm for Improving Data Security

In this technique they describe about a new cryptography algorithm which is based on block cipher concept. In the algorithm they have used logical operation like XOR and shifting operation. In this technique they used a random number for generating the initial key, where this key will use for encrypting the given source file using proposed encryption algorithm with the help of encryption number. Basically in this technique a block based substitution method will use. In this technique they will provide for encrypting message multiple times. Initially that technique is only possible for some files such as MS word file, excel file, text file.

2.2 Secure Data Retrieval Based on Ciphertext Policy Attribute-Based Encryption (Cp-Abe) System for the Dtns

Mobile nodes in military environments such as a battlefield or a hostile region are likely to suffer from intermittent network connectivity and frequent partitions. Disruption-tolerant network (DTN) technologies are becoming successful solutions that allow wireless devices carried by soldiers to communicate with each other and access the confidential information or command reliably by exploiting external storage nodes. Some of the most challenging issues in this scenario are the enforcement of authorization policies and the policies update for secure data retrieval. Ciphertext-policy attribute-based encryption (CP-ABE) is a promising cryptographic solution to the access control issues. However, the problem of applying CP-ABE in decentralized DTNs introduces several security and privacy challenges with regard to the attribute revocation, key escrow, and coordination of attributes issued from different authorities. In this paper, we propose a secure data retrieval scheme using CP-ABE for decentralized DTNs where multiple key authorities manage their attributes independently. We demonstrate how to apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the disruption-tolerant military network.

III. DESCRIPTION OF RSA ALGORITHM

Keeps security in sending secrets message using RSA Algorithm implemented through web service: The RSA algorithm can be used for both public key encryption. Its security is based on the difficulty of factoring large integers. RSA algorithm segregated into two parts:

Encryption of secret message: Rather represent the secret message as an integer directly, we generate a random session key and use that to encrypt the secret message with a conservative, much faster symmetrical algorithm like Triple DES. We then use the much slower public key encryption algorithm to encrypt just the session key.

Decryption encrypted secret message: The sender A then transmits a message to the recipient B in a cipher text format. The recipient B would extract the encrypted session key and use his private key (n,d) to decrypt it. He would then use this session key with a conventional symmetrical decryption algorithm to decrypt the original message. Typically the transmission would include in secret message details of the encryption algorithms used (CIPHER Text). The only secret necessary to be kept, as always, should be the keys.

Session Key: A session key is decryption and an encryption key that is randomly generated to ensure the security of a communications session between a user and another computer or between two computers.

Qubit Generation: To get the secret key and random string, then change it into hex-code and then convert it into binary, find the least bit of the two binary values and get the quantum bit of 0 and 1.

IV. PROPOSED WORK

In this paper I am proposed a block based symmetric cryptography algorithm. In this technique I have used a pseudo random prime number and exponential values of random number for generating the initial key using session key method, where this key uses for encrypting the given source file using RSA algorithm. Our proposed system using 512 bit key size with combination of alphanumeric method to encrypt a text message. It will be very difficult to find out two same messages using this parameter. To decrypt any file one has to know exactly what the key block and to find the random blocks with the combination of alphanumeric numbers, theoretically one has to apply 2256 trail run and which is intractable. But initially that technique is not possible to find the combination of alphanumeric methods using 2256 trail run.

4.1. Session Key Generation Steps

- It is a shared secret key which is used for encryption and decryption.
- The size of session key is 512 bits with combination of alphanumeric characters.
- This session key is generated from pseudo random prime number and exponential values of random number.

4.2. Proposed Algorithm

- Get the secret key, then convert it into hex-code and then convert it into binary.
- Find the least bit of the two binary values and get the quantum bit of 0 and 1.
- Generate the quantum key using the qubit and session key this depends on the qubit.

Combinations,

1. If (Last two bit = 0) then 1/√2(p[0] + p[1]).
2. If (Last two bit = 1 && 0) then 1/√2(p[0] - p[1]).
3. If (Last two bit = 0 && 1) then p[0].
4. If (Last two bit = 1) then p[1].

- Encrypt the session key by using the master key and store all the values.
- Key distribution center distributes the original session key and qubit to the sender for Encrypting the message.
- Key distributor center also distributes the key and qubit to the corresponding receiver to Decrypt the received messages.

V. SAMPLE RESULT

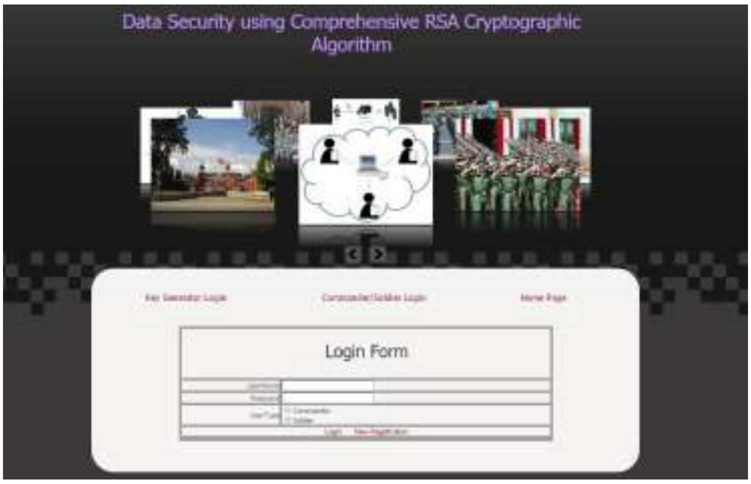
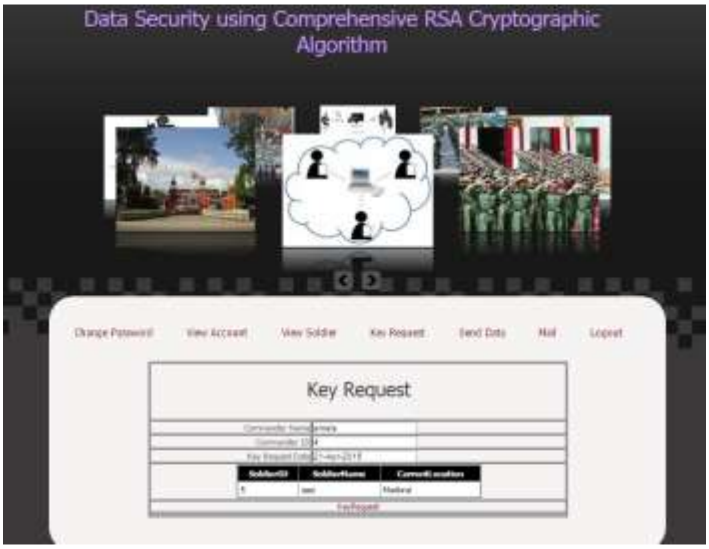


Fig 3 : Login for User



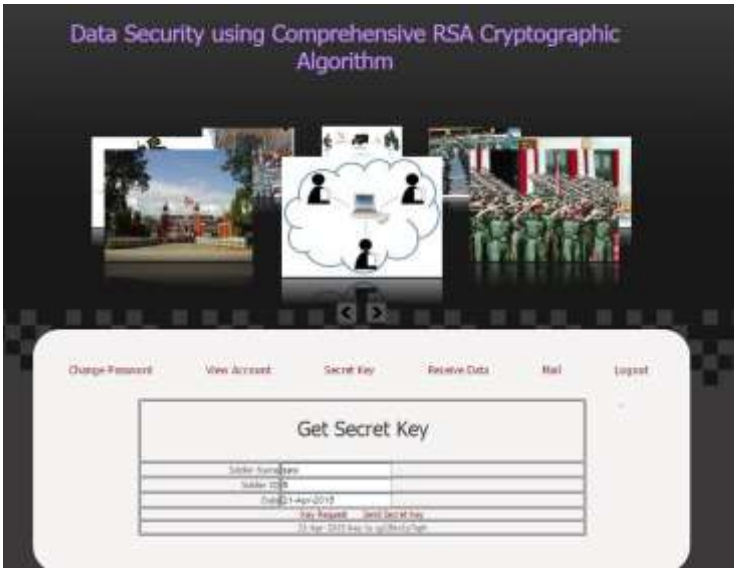
Key Request

Commander Name: [illegible]
Commander ID: 4
Key Request Date: 21-Apr-2015

SoldierID	SoldierName	CurrentLocation
5	[illegible]	Madurai

KeyRequest

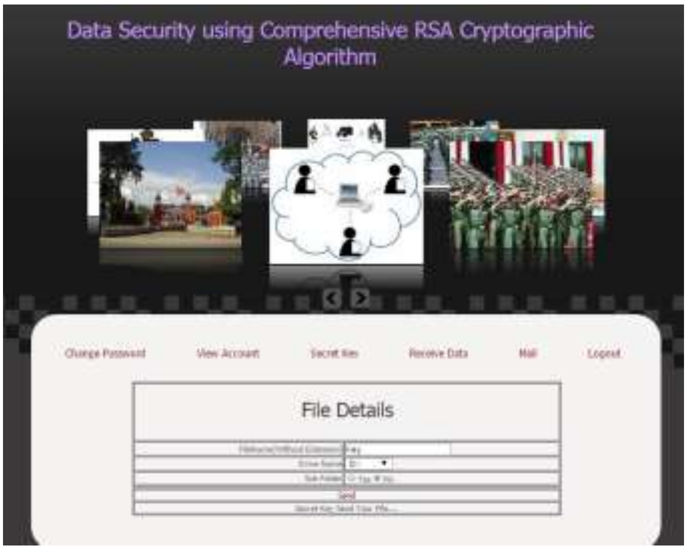
Fig 4 Secret Key Request


Data Security using Comprehensive RSA Cryptographic Algorithm
Change Password
View Account
Secret Key
Receive Data
Mail
Logout

Get Secret Key

Soldier Name: [illegible]
Soldier ID: 5
Date: 21-Apr-2015
Key Request Send Secret Key
21-Apr-2015 Key is [illegible]

Fig 5 Get Secret Key from Key Generator

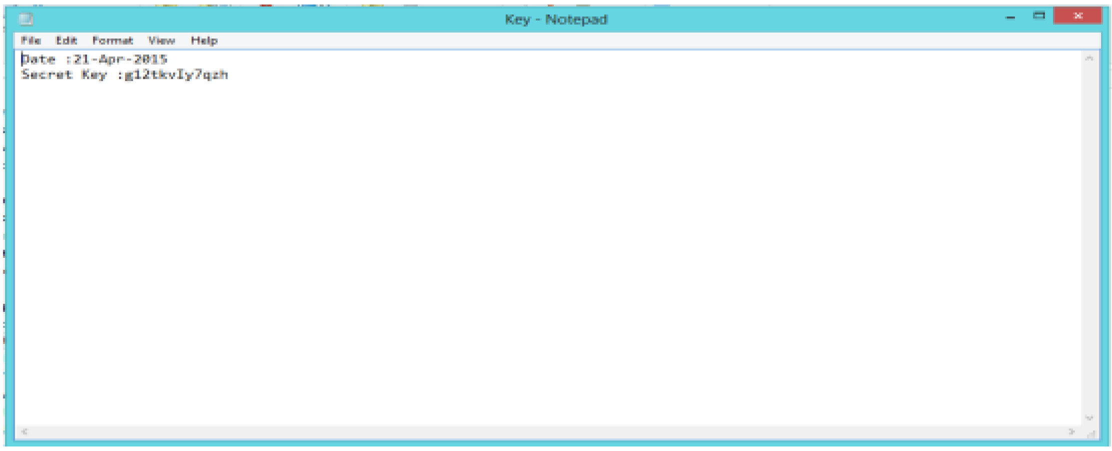

Data Security using Comprehensive RSA Cryptographic Algorithm
Change Password
View Account
Secret Key
Receive Data
Mail
Logout

File Details

FileName(Without Extension): Key
Drive Name: D:
Sub Folder: [illegible]
Send
Secret Key Send Your File....

Fig 6 Get Secret Key in File Format

Secret Key – Send to File



```
Date :21-Apr-2015
Secret Key :g12tkvIy7qzh
```

Fig 7 Get Secret Key in File Format with Combination of Alphanumeric Method

VI. CONCLUSION

In this proposed technique is especially for block cipher method and it will take less time of the file size is large. The important thing of our proposed method is impossible to break the encryption algorithm without knowing the exact key value. We ensure that this encryption method can be applied for data encryption and decryption in any type of public applications for sending confidential data.

REFERENCES

[1] DriptoChatterjee, JoyshreeNath, SubadeepDasgupta, AsokeNath "A new Symmetric key Cryptography Algorithm using extended MSA method: DJSA symmetric key algorithm" published in 2011 International Conference on Communication Systems and Network Technologies, 987-0-7695-4437-3/11 $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. 2009.81.

[3] Symmetric key cryptography using random key generator A.Nath, S.Ghosh, M.A.Malik, Proceedings of International conference on SAM-2010 held at Las Vegas (USA) 12-15 JULY, 2010, Voll-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 Published by Springer-Verlag. [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 "Simple Encryption/Decryption Application" published in International

[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. MonirHossain 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 DOI 10.1109/SNPD.2008.101 IEEE 2008.

[11] [Rijn99]JoanDaemen and Vincent Rijmen, AES submission document on Rijndael, Version 2, September 1999**.**

[12] SwatiKamble, “Advance Cryptography Algorithm for Improving Data Security” National Conference On Research Trends In Electronics, Computer Science & Information Technology And Doctoral Research Meet, Feb 21st & 22nd, 2014. NCDRM-2014.

[13] Dr.AnandaRao.G, Srinivas.Y, VijayaSekhar.J, Pavan Kumar.ch “ Three Party aunthentication key distributed protocols using implicit and explicit Quantum Cryptography.” Indian journal of Computer Science and Engineering(IJCSE), ISSN:0976-5166.