*Available online at http://www.ijcrls.com*

*International Journal of Current Research in Life Sciences*
*Vol. 07, No. 02, pp.1088-1092, February, 2018*

**ISSN: 2319-9490**

# RESEARCH ARTICLE

# AN IMPLEMENTATION OF KEY WRAPPING FOR A USER IN A GROUP USING SPONGE FUNCTION BASED ON PKCS

**Kuduganti Venkata Rao, *Marada Srinivasa Rao and Pulavarti Vasavi**

Computer Science and Engineering, Vignan's Institute Of Information Technology, Visakhapatnam, India

Received 09th December, 2017; Accepted 20th January, 2018; Published Online 28th February, 2018

## ABSTRACT

Authenticated Encryption (AE) is a symmetric key cryptographic scheme that aims to provide both confidentially and data integrity. This project presents a novel approach a (key distribution) for secret message communication among a group (g) using wrapping technique. In order to increase security to distribute secret message (key) and a generate a key to distribute we introduce a wrapping technique in sponge (where as even absorbing and squeezing function are also used). In this project implementation of secret key distribution is to be done in a group of server-client technology using sponge function. In this process a sponge tool batch file installed in the server. The server will distribute or communicate the secret message to client based on one to one or one too many mapping. With the help of the sponge tool a message has been encrypted and distributes to respective clients. In the client side the decryption batch file to be installed to be verification of secret message authentication. We calculate the time complexity and space complexity for message cryptosystem and generate one time password for key communication which gives more security and can stop hackers form hacking the data.

***Key words:*** Sponge function, RSA algorithm, Group communication, Encryption and decryption, Key wrapping, Secret key generation (OTP).



**Citation: Kuduganti Venkata Rao, Marada Srinivasa Rao and Pulavarti Vasavi, 2018.** "An implementation of key wrapping for a user in a group using sponge function based on PKCS" *International Journal of Current Research in Life Sciences*, 7, (02), 1088-1092.

## INTRODUCTION

In 1898 Madison Square Garden that allowed secure communication between transmitter and receiver. One of the most famous systems of secure communication was the Green Hornet The security of data transmission is a vital problem in communication networks. A communication system is reliable as long as it provides high level of security. Usually, users exchange personal sensitive information or important documents. In this case; security, integrity, authenticity and confidentiality of the exchanged data should be provided over the transmission medium. Nowadays, internet multimedia is very popular a significant amount of data is exchanged every second over a non secured channel, which may not be safe Therefore, it is essential to protect the data from attackers Cryptography is the science of keeping the transmitted data secure. It provides data encryption for secure communication. The encryption process is applied before transmission, and the decryption process is applied after receiving the encrypted data the information hiding process is applied before transmission and the extraction process is applied after receiving. Cryptographic algorithms are classified as symmetric key algorithm and public key algorithm. Symmetric key algorithm uses the same key for encryption and decryption, while public key algorithm uses different keys for encryption and decryption. In the context when many applications are expected to run over the Internet (Varaprasad *et al.,* 2013). Need for security in computing and communication became a necessity. To overcome this we go for the Secure Key distribution in a group using sponge function by using key wrapping technique. In this my project is to give the high level data accessing in communicating the message between user in the group by using key wrapping technique based on sponge function using client server technology (Saleh Saraireh, 2013).

**Group Communication Systems:** Group communication systems are distributed messaging systems that enable efficient communication between a set of processes logically organized in groups and communicating via multicast in an asynchronous environment. group communication systems is achieving agreement about group membership views and about the order of delivering messages, between multiple participants, communicating in an asynchronous environment with failures. Group communication systems have been built around a number of different architectural models, such as peer-to-peer and client-server (Venkata Rao, 2017).

**Existing System:** In existing system many applications, a group of members are required generate digital signature. The user encrypt the data to send a data to particular group with

***Corresponding author:*** **Marada Srinivasa Rao,**
Computer Science and Engineering,Vignan's Institute OF Information Technology, Visakhapatnam, India

respective of group public key. The message is decrypted by end user by the respective group members using group private key the computational cost for Signature generation and verification is high. In these system client will encrypt the message and send to the receiver the receiver will decrypt the message from client.

**Proposed System**

The computational cost is reduced when compared to other schemes. We have applied the multi signature in a simple application for sending group messages. Implement communication by using technique called as one –one and one-many communication in network for message communication by using sponge function with technique of key wrapping Compute the time complexity and space complexity for message cryptosystem and generate one time password for key communication which gives more security and can stop hackers form hacking the data To implement a Key wrapping scheme easily delivers the security level of 128 bits or higher with the master key of the same length. In this proposed system we have to generate the otp it its very useful for authentication so we have to implement the otp through Gmail.

**Advantages proposed system**

Single and group user message authentication system with key distribution using sponge function. Key distribution can be done to the specific users in the group for data communication by using mapping key. Security access is more provided using OTP (one time password technique).

**Analysis of project methods**

The block diagram illustrate the complete process of the project .It consiststing of three phases they are

**(i) Connection establishment:** In this process user has to be registered in to the login page .He can be registered into any of the group present in the registration page .In this registration page the user will fill the details in registration form after that the secret key generated and send to the user registration mailed .another phase is login page we are going to enter the user id, password and secret key which is generated after that the user can get into the group successfully. The following figure 1 shows the architecture of my project the below are the steps for procedural implementation of my project.

**(ii) Key Generation Using Rsa on Encryption Using Sponge function and Key Wrapping:** Now in the sender side a user sending data box where we enter the message that need to be send to the receiver and generate a public key and private key by using rsa algorithm and encrypted text also generated using rsa algorithm.

**a) Applying of Sponge and Key Wrapping Technique:** The encrypted text is large in size so for this we use sponge function on the encrypted text and generate the reduced size encrypted text and key wrapping technique is also applied on the generated reduced encrypted text to get a wrap key. This wrap key is stored in the server. After that admin login page where the admin login into server he has the authority to data access through the admin home page .we can the select the require group and members in the group to the send the message to send the encrypted data and wrap key also to the user mail.

**(iii) Decryption process:** In decryption side user need to enter the wrap key along with encrypted text. The server validate the receiver by verifying its signature after that it generate the public key. By using the public key it unwraps the wrap key after that private key will generated to obtained the original message

**Proposed Architecture**
**Related work**

**Sponge Function**

Distributing the key among a set of legitimate users, guaranteeing the secrecy of the key is a central issue in Cryptography. Sponge functions are the more secure and are generalized cryptographic hash functions to generate the key. In this case sponge function is used to generate the public key of the group taking all the private keys of the group users. Sponge construction is a repetitive function to provide a desired length output from a variable length input.

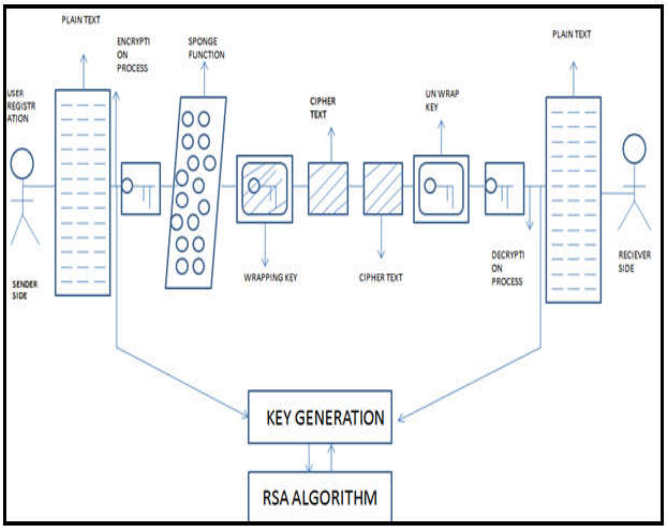



**Figure 1.**

**Sponge construction**

The sponge construction is a simple iterated construction for building a function $F$ with variable-length input and arbitrary output length based on a fixed-length transformation or permutation $f$ operating on a fixed number $b$ of bits. Here $b$ is called the width. The sponge construction operates on a state of $b = r + c$ bits. The value $r$ is called the bit rate and the value $c$ the capacity. First, all the bits of the state are initialized to zero. The input message is padded and cut into blocks of $r$ bits. The sponge construction then proceeds in two phases: the absorbing phase followed by the squeezing phase.

i. In the absorbing phase, the $r$-bit input message blocks are XO Red into the first $r$ bits of the state, interleaved with applications of the function $f$. When all message blocks are processed, the sponge construction switches to the squeezing phase.
ii. In the squeezing phase, the first $r$ bits of the state are returned as output blocks, interleaved

iii. With applications of the function *f* .The number of output blocks is chosen at will by the user.

The last *c* bits of the state are never directly affected by the input blocks and are never output during the squeezing phase.

**Key wrapping:** Using this key wrapping we can generate a key that is called as wrapping key which is used to wrap the original data sent by the sender so by doing this we can give data integrity and authentication to the data .the receiver also receive the wrap key to avoid hacking by the third party .the key generated is secured that even the third party cant trace the original data.

**Key wrapping algorithm**

The inputs to the key wrapping process are the KEK (key encrypted key) and the plaintext to be wrapped. The plaintext consists of n 64-bit blocks, containing the key data being wrapped. The key wrapping process is described below.

Inputs: Plaintext, n 64-bit values {$P_1$, $P_2$,,,,,Pn}, and Key, K (the KEK).

Outputs: Cipher text, (n+1) 64-bit values {$C_0$, $C_1$,…, $C_n$}.

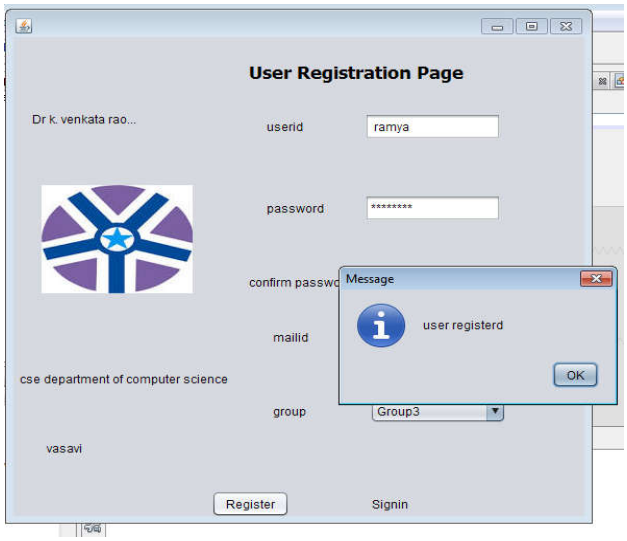
1) Initialize variables.

Set A0 to an initial value (see 2.2.3)
For i = 1 to n
R[0][i] = P[i]

2) Calculate intermediate values.

For t = 1 to s, where s = 6n
A[t] = MSB(64, AES(K, A[t-1] | R[t-1][1])) ^ t
For i = 1 to n-1
R[t][i] = R[t-1][i+1]
R[t][n] = LSB(64, AES(K, A[t-1] | R[t-1][1]))
3) Output the results.
Set C[0] = A[t]
For i = 1 to n
C[i] = R[t][i]

**Output screens**

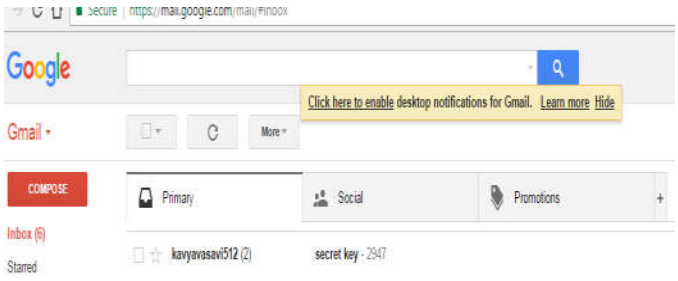



**User Registration page**

**Registration page**

In this process user has to be registered into the login page .the user can be registered into any of the group present in the registration page .In this registration page the user has to fill the user id password Gmail id and also group. After that pop box appears "user registered".

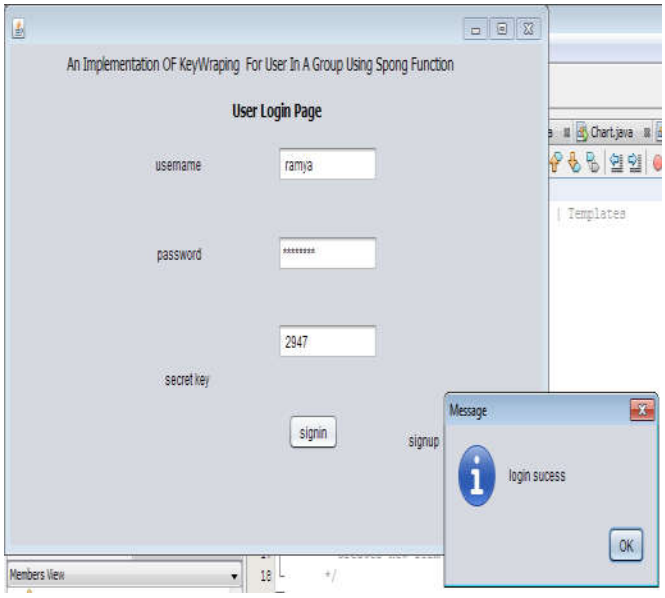
**Secret key generation:** After complete the registration the secret key will generated and sent to the user registration mail id as shown in the below screen shot




**Secret key Generation**

**user login**

In this below screen shot client need to login for communication between groups .we are going to enter the user id and password and secret key which is generated. After filling the user details then pop box will appear as the user login successfully

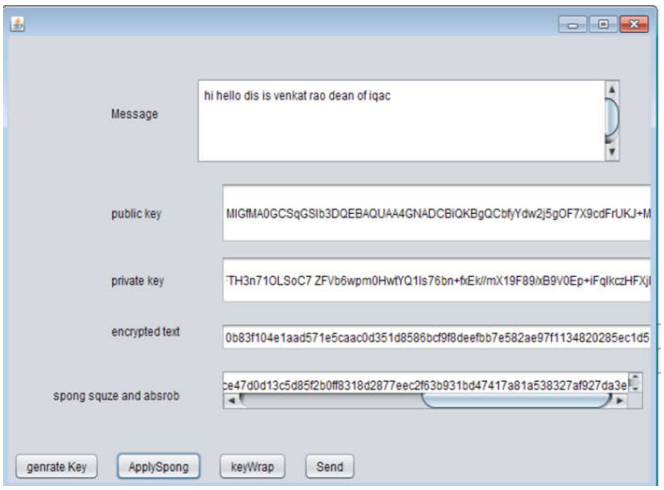



**Login Success**

**Encryption process**

**Sender side**

In the below screen shot describe user want to enter the plain text after that the generate the public and private keys are generated by using rsa algorithm after that encrypted text will generated after that we use sponge technique on the encrypted text and generate a reduced size encrypted text wrapping technique applied on the generated reduced encrypted text to get a wrap key and this wrap key is stored in the server

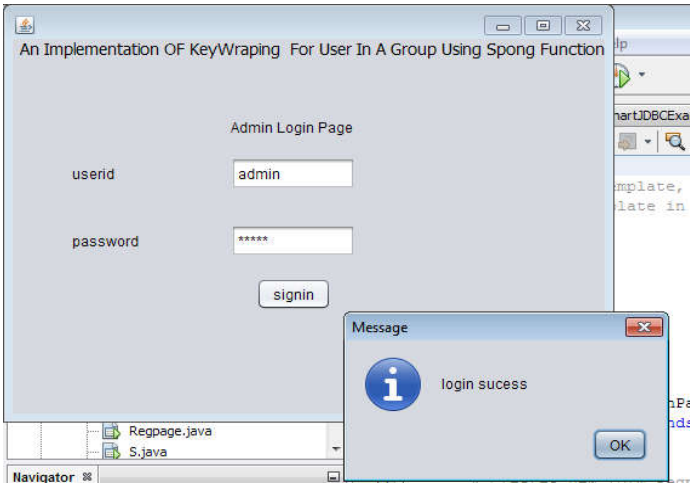



**Output of sender**

**In this below screen shot shows the generated**

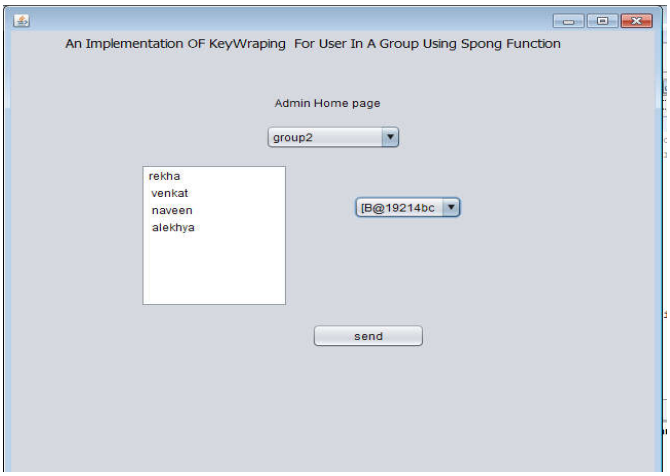
## Admin Login Page

In this screen shot admin can login into the server . He his the authority to data access. The admin give to username as admin and password as admin then admin will login successfully in to server.




**Admin login page**

**Admin Homepage:** In this screen shot the admin select the user and group and also select the wrap key and click on send then wrap key will send to the user Gmail.




**Admin Home Page**

## One to One Communication

In this admin log in page admin can select the one user is vasavi and wrap key then click on send after that wrap key and encrypted text will send to the vasavi Gmail id..In the below screen shot shows the one to one communicating the data and output, otp.


**One To One Communication**

## Group communication

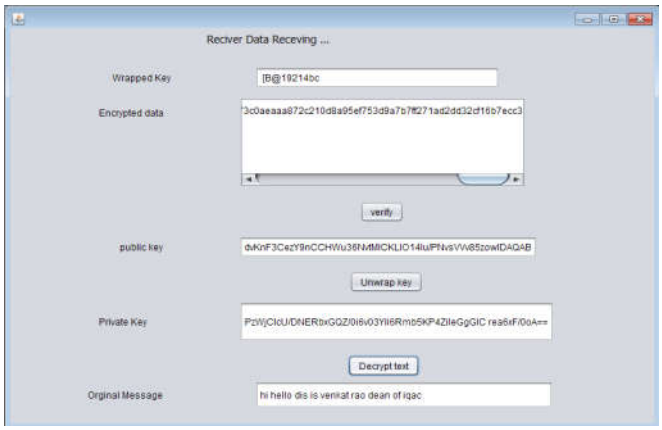
## DECRYPTION PROCESS

## Receiver Side

In the screen shot which user get the wrap key and encrypted text that user will enter into the given receiver data box and verify from the server the user is authorized or not after the verification is completed from server the public key is un wrapped with wrap key after that private key will generate and decrypt the message by using user private key finally user get the original message.

## Output of Receiver

In this screen shot shows the time taken to process the data and space of encrypted data also showed

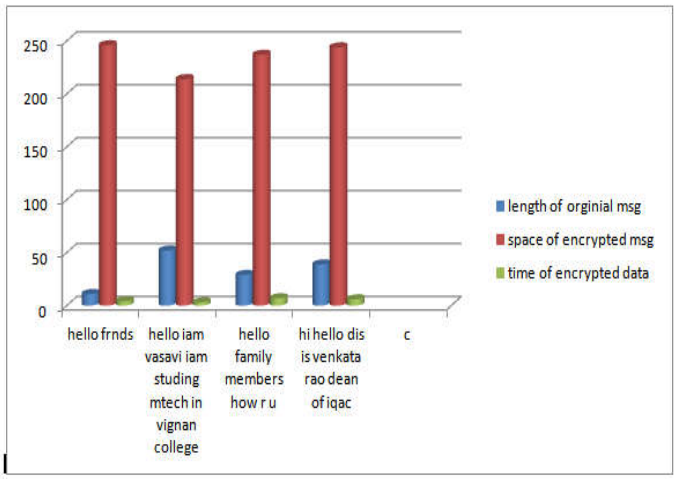



**Receiver side**


**Receiver Side Output**

## RESULT ANALYSIS

**Time and Space Complexity Graph:** Here in this system i have considered 4 different sized data types and calculated time and space complexities with the 3 factors such as: Length of original message, Space of Encrypted message, and Time of Encrypted data. The below table shows the calculated result analysis for the data types taken.




| Original Message | Length of Original Message | Space Of Encrypted Data | Time OF Encrypted Data |
|---|---|---|---|
| Hello frnds | 11 | 246 | 4 |
| Hello iam vasavi iam studying mtech in vignan college | 52 | 214 | 3 |
| Hello family members how r u | 29 | 237 | 7 |
| Hi hello dis is venkata rao dean of iqac | 39 | 244 | 6 |

**Security Issues:** Security and confidentiality are the top most concerns of the client. Quality issues refer to how reliable, available and robust should the system be, while developing the proposed system the developer must be able to guarantee the reliability transactions so that they will be processed completely and accurately. The ability of system to detect failures and recovery from those failures refers to the availability of system.

### Conclusion

Using sponge function a secure communication has been established in a group using key wrapping technique .As mentioned above by using a key wrapping technique it gives more security for large scale communication of data with multi verification. By using key wrapping technique each and every message can be transmitted is secured knowledge of third party .In this system third party cannot access the data for the messages delivered between the members of the group, the project ensures confidentiality, authenticity, integrity. As there is a very important need for Secure Group Communications by many networking applications also on the internet, the project has many network applications such as teleconferencing, information services, distributed interactive simulation, collaborative work, and group meetings**.** Information Services is a system most commonly used on the internet these days where information on any subject is updated by the server to the peers registered to it. Distributed Interactive Simulation (DIS) is an open standard for conducting real time platform level war across multiple host computers and is used in military organizations but also by other agencies such as those involved in space exploration and medicine. This work can be extend in Data mining and Data ware housing, Image processing. We can increase the performance and reduce the time complexity of the process. As the security aspects are increasing day by day, this factor helps in the group messaging in a broad manner. Hence privacy increases and this work is highly implemented in all the domains.

### Future Work

In future we can expand the scope of the project for communicating digital information more securely (video, audio, transmission, picture recognition) among n number of groups. In future this project can also be expanded to transmit files among the users in the group.

## REFERENCES

"The cryptography sponge function" family Guido Bertoni, Joan Daeme, Michaël Peeters and Gilles Van Assche.

Cristina Nita-Rotaru, 2002. "High-Performance Secure Group Communication". Advanced Encryption Standard (AES) Key Wrap Algorithm "j.schaad,soaring hawk category informational hously, 2002.S.

Dr Venkata Rao, K., Eluri Nageswara Rao, 2017. "Secret Message Secure Communication in A Group Using Pkcs Based on SpongeFunction", *American Journal of Engineering Research,* Volume-6, Issue-1, pp-256-262.

Matthew Kelly, Alan kaminsty "Customizable;e sponge based authenticated Encryption using 16- bit s- boxes.

Saleh Saraireh, "a secure data communication system using cryptography and steganography" *International Journal of Computer Networks & Communications (IJCNC),* Vol.5, No.3, May 2013.

Varaprasad S., K. Venkata Rao, and P.S. Avadhani. "A Novel Approach to Communicate Secret Message between Users Using Sponge Function Technique on NTRU", *Internat. J. of Sci. and Eng.,* Vol. 4(2)2013:44-51, April 2013.

*******