International Journal of Advanced Research in Education and TechnologY(IJARETY)

| ISSN: 2394-2975 | www.ijarety.in| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 1, Issue 3, November 2014 ||

Hybrid Key Cryptography: A Tool for Security

Ashish Agarwal[2], Anurag Katiyar[2], Shubham Garg[2], Shudhanshu Yadav[2]

Department of Computer Science & Engineering, G.L.Bajaj Institute of Technology & Management, Greater Noida, Uttar Pradesh, India[2]

ABSTRACT: The vulnerability of information to the security threats has always been the topic of grave concern for the experts in this field. It is because of the consistent efforts by the concerned people in this domain that have led to the generation of multiple methodologies in order to counter interact with the suspected security attacks. For the lame users who are unaware of the possible attack(s) to their information demanding utmost secrecy, are left with no choice when bullied by the playful activities representing unethical attempts to break the confidentiality of their communication. Albeit techniques have been developed, many are in developing phase(s), the upsurge of new attack(s)/threat(s) urges for the need of much more strengthened tool(s) to deal with them. In a row of such efforts, we have heard the separate class of cryptography named hybrid cryptography. We have tried to imply our idea in the former with no intention to violate the essence of the technique. We have focussed on to render considerable amount of security to the method(s) used in hybrid cryptography as one of its constituents.

KEYWORDS: Hybrid Cryptography, Security Threats, Private Key Cryptography, Public Key Cryptography, Key

I. INTRODUCTION

"Hybrid Cryptography", as perceptual comprises of two individual terms namely 'Hybrid' and 'Cryptography'. Cryptography [9] is itself made on two pillars namely Encryption and Decryption. It is mainly of two types i.e.; Symmetric key cryptography and Asymmetric key cryptography. The word 'hybrid' [3]implies the mixture of two primarily known, above mentioned types of cryptography i.e.; dominating the respective features of both kinds into one system altogether to increase the strength of encryption process [2] and hence its name as hybrid.

Thus, Hybrid Cryptography= Symmetric key Cryptography + Asymmetric Key Cryptography Therefore in order to justify this merger and the possibility of applying such system to shield against the security breaches, we need to understand the features of each one of them individually with respect to the hybrid cryptography.

II. CONCEPT

A Hybrid Encryption scheme is a mixture which focuses primarily on blending together the facilities of asymmetric encryption with the effectiveness of symmetric encryption [8].
Hybrid encryption can be accomplished with data transfer using unique session keys along with the symmetric encryption.
Symmetric key cryptography utilises a scheme called as data encapsulation schemei.e.the focus is laid on how securely our data may be rendered confidential mode of communication between its sender and receiver by hiding it with the single sharable key called as secret key[2] or private key. Since the symmetric methodology requires only one sharable key, hence its name symmetric [4]. The procedure of the same may be illustrated using notations as follows:
Sender, 'S' sends a message, 'M' to the receiver, 'R'
Hence, encryption, 'E' performed at the sender's end i.e.
Key, K →message, M➔E
We can think this step as a locking of the data whose unlocking key is K.
Now, when this encrypted data is received at the receiver's end, it has to be decrypted in order to obtain the data using the same key, 'K' which is sharable i.e.; same for both sender and receiver.
Hence, decryption, 'D'performed at receiver's end i.e.
Key, K→encrypted data, E➔message, M
As can be predicted that, for the short length message(s), the above procedure is very efficient, but when it comes to be applied for lengthy message(s), it may not be able to maintain that magnitude of efficiency. It is because of the single key being exchanged between both the parties that may get cracked easily. Hence the idea of encrypting the encrypted data [5] i.e. double encryption came into existence.

| ISSN: 2394-2975 | www.ijarety.in| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 1, Issue 3, November 2014 ||

Before we move further we need to understand the basic functioning of Asymmetric key cryptography. Asymmetric key cryptography, as the name suggests employs the usage of two different keys for the process of encryption and decryption(R.S.A. algorithm, for example) [6]. The application of two separate keys makes it worth preferred to previous methodology (ies). Therefore, it is based on the scheme called as key encapsulation scheme i.e.how key is safeguarded using other key in order counter the possibility(ies) of potential threats to the confidentiality of the process of exchange. We are aware of the functioning of asymmetric key cryptography i.e. it uses two different keys namely public key and private key for both the encryption and decryption process. The public/private key of receiver/sender can be used to encrypt the data(here already encrypted by means of symmetric key technique) and can be decrypted at receiver's end using private/public key of receiver/sender respectively.

It is known that the asymmetric encryption decelerate the encryption process, but with the incorporation of symmetric key both of these encryption processes are strengthened.

III. WORKING

Let us suppose the encrypted data obtained from applying symmetric key algorithm be E. Now, we can further encrypt it, called as double encryption, E', using the public key of receiver, R say P or private key of sender, S say P' i.e.
Double Encryption at the sender's end is-

Public Key, P→encrypted data, E➔E'

Or

Private Key, P'→encrypted data, E➔E'

Now, when this double encrypted data reaches the receiver's end, it has to be decrypted prior to the decryption of message, M using key, K. The outer layer of encryption can be decrypted(may be called as first unfolding) using the private key of receiver, R say P" or public key of sender, S say P"' i.e.
First unfolding at receiver's end is-

Private Key, P"→double encrypted data, E'➔encrypted data, E

Or

Public Key, P"'→double encrypted data, E'➔encrypted data, E

The next step to obtain the original message, M is to simply decrypt it using shared symmetric key, K. This two-step unfolding i.e. two levels of encryption and equal number decryption using two different methodologies yields a strengthened system worth applicable to enhance the feature(s) that guarantee the successful application of cryptosystem to secure communication [12] meeting the purpose capable of countering attacks that may prevail in its way.

Thus, we may represent the wholefunctionality of hybrid cryptographyby using a simple diagram as follows:-

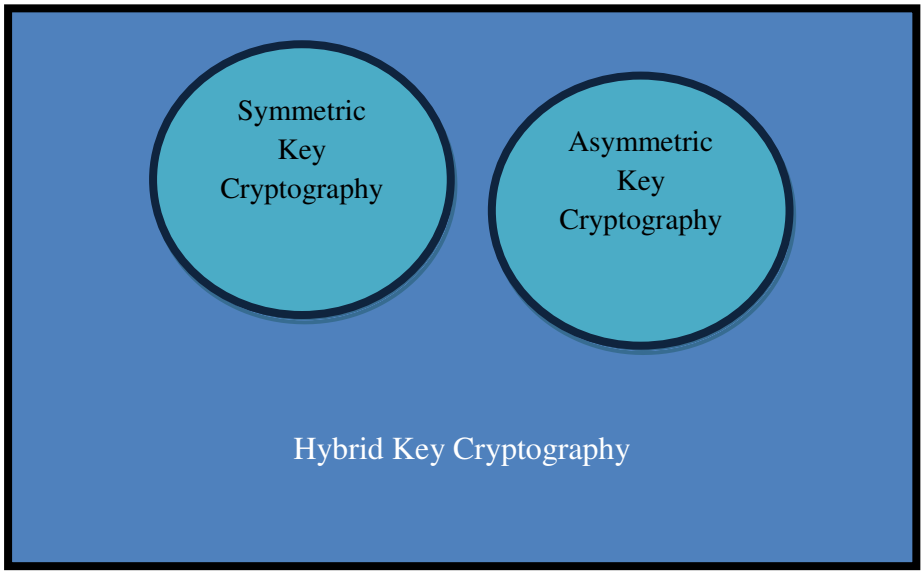

Figure 1: Representing the functionality of Hybrid Key Cryptography

| ISSN: 2394-2975 | www.ijarety.in| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 1, Issue 3, November 2014 ||

The obvious advantage of merging two different methodologies into one is the enhanced capacity to fight against security loopholes and render robust communication medium that safeguards the user(s) against inappropriate security issues concerned with their important information.Working together both symmetric and asymmetric complement each other and intensify their features. We have considered RSA algorithm[1] as one of the most preferred asymmetric algorithms and so its application in hybrid cryptography. However, slight modifications in RSA algorithm can be added in its working since asymmetric algorithms are based on mathematical computational complexities.The idea[1] is to enhance the security [7] of the channel that is used to transmit the key between two communicating parties.

Example:
Here we look at an example which would provide a detailed overview of how data encapsulation is carried out.
We take a conversation which consists of two parties Kate and Alex,
Before Kate sends the message to Alex, She needs to encrypt it:
The Encryption process consists of following steps,

1. Kate is required to acquire the public key of Alex.
2. Now Kate generates a new symmetric key for the data encapsulation strategy.
3. Then Kate uses this newly generated symmetric key to encrypt the message through it.
4. With the help of Alex's public key, Kate now encrypts the symmetric key under the key encapsulation strategy.
5. Finally, Kate sends both the encryptions over to Alex.

Once these encryptions successfully received by Alex, He then needs to perform the decryption process to retrieve the actual message.

1. Now Alex uses his own private key to decrypt the symmetric key present in the key encapsulation segment.
2. Then he uses this symmetric key to decrypt the original message present in the data encapsulation segment.

IV. FURTHER DISCUSSION

With the advent of new security threats, there is need to work in parallel to diffuse such unwanted attempts that tend to create fear and breach the confidentiality of the communication process. The concept of hybrid cryptography is not new in today's context indeed there is a need to add more security features in order to attain our targets by allowing unobstructed medium. Here, we have considered RSA algorithm to understand the asymmetric key method, there may be other methods too available and can be taken as a potential area(s) of improvement. There exist(s) vast opportunity (ies) in modifying the underlying principles [10] used for implementing the hybrid cryptography, also called as mixed key cryptography.

V. CONCLUSION

It is not always necessary to design new methodology or write absolutely new algorithm but we can try to think, if feasible, to make changes in the already available tools. So we have tried the same in our attempt to further strengthen the widely applicable class of cryptography named hybrid cryptography by introducing a certain level of modification. There may be requirement(s) to add/remove certain working method(s) [11] but the overall essence of technique(s) needs to be preserved. Moreover, the running time and space requirements of used algorithm(s) need to be consistently improved based on its/their application(s).

REFERENCES

[1] Neha Tyagi, Ashish Agarwal, Anurag Katiyar, Shubham Garg, Shudhanshu Yadav, "Protection of Key in Private Key Cryptography" published by "International Journal of Advanced Research", Volume 5, Issue 2, Feb 2017.
[2] Arpit Agrawal, Gunjan Patankar,"Design of Hybrid Cryptography Algorithm for Secure Communication" published by "International Research Journal of Engineering and Technology", Volume 3 Issue 1, Jan2016.
[3] Meenakshi Shankar, Akshay.P, "Hybrid Cryptographic Techniques Using RSA Algorithm and Scheduling Concepts" published by "International Journal of Network Security & Its Application", Volume 6, Issue 6, Nov2014.
[4] Vishwa Gupta, Gajendra Singh,Ravindra Gupta,"Advance cryptography algorithm for improving data security" published by "International Journal of Advanced Research in Computer Science and Software Engineering", Volume 2, Issue 1, Jan 2012.

| ISSN: 2394-2975 | www.ijarety.in| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 1, Issue 3, November 2014 ||

[5] Prakash Kuppuswamy, Saeed Q. Y. Al-Khalidi, "Hybrid Encryption/Decryption Technique Using New Public Key and Symmetric Key Algorithm", by"Department of Management Information Systems, College of Commerce National Chengchi University & Airiti Press Inc.", Vol. 19, Issue 2, Mar 2014.

[6] Ravindra Kumar Gupta, Parvinder Singh, "A New Way to Design and Implementation of Hybrid Crypto System for Security of the Information in Public Network" published by"International Journal of Emerging Technology and Advanced Engineering", Volume 3, Issue 8, Aug 2013.

[7] Dr. Vivek Kapoor, Rahul Yadav, "A Hybrid Cryptography Technique to Support Cyber Security Infrastructure", published by"International Journal of Advanced Research in Computer Engineering & Technology", Volume 4, Issue 11, Nov 2015.

[8] Swati Kashyap, Er. Neeraj Madan, "A Review on: Network Security and Cryptographic Algorithm", published by "International Journal of Advanced Research in Computer Science and Software Engineering", Volume 5, Issue 4, Apr 2015.

[9] Prof K.Govinda, Dr.E.Sathiyamoorth, "Multilevel cryptography technique using graceful codes" published by, "Journal of Global Research in Computer Science", Volume 2, Issue7, Jul 2011.

[10] Prof. Mukund R. Joshi, Renuka Avinash Karkade, "Network Security with Cryptography", published by "International Journal of Computer Science and Mobile Computing", Volume 4, Issue 1, Jan 2015.

[11] Maricel O. Balitanas, "Wi Fi Protected Access-Pre-Shared Key Hybrid Algorithm", published by"International Journal of Advanced Science and Technology", Volume 12, Nov 2009.

[12] Amrita Jain,Vivek Kapoor, "Policy for Secure Communication using Hybrid Encryption Algorithm", published by"International Journal of Computer Applications" Volume 125, Issue 10, Sep 2015.