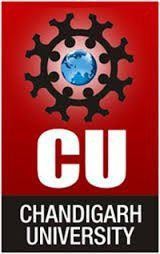
**HYBRID CRYPTOGRAPHY**

Submitted in partial fulfillment of the requirements for the award of degree of

**BACHELOR OF ENGINEERING** **IN**

**COMPUTER SCIENCE & ENGINEERING**



**Submitted to:**

**SHIKHA ATWAL**

**Submitted By:**

**YUKTI GOYAL 18BCS1838**

**PRADIPTA SARKAR 18BCS1854**

**MIRTUNJAY GUPTA 18BCS1843**

**SHUBHAM SHUKLA 18BCS1848**

**DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING**

**Chandigarh University, Gharuan**

**August 2019**

**INTRODUCTION**

Cryptography enables the user to transmit confidential information across any insecure network so that it cannot be used by an intruder. Cryptography is the process that involves encryption and decryption of text using various mechanisms or algorithms. A cryptographic algorithm is a mathematical function that can be used in the process of encryption and decryption. Encryption is the process of converting the plain text into an unreadable form called a cipher text. This unreadable form cannot be easily understood by an intruder and sent across the insecure media. Decryption is the process of converting this unreadable form back into its original form, so that it can be easily understood by the intended recipient. Many algorithms exist for encryption that can be categorized into symmetric and asymmetric encryption. In symmetric-key cryptography, also called conventional cryptography or secret-key encryption, one key is used both for encryption and decryption. Examples include DES and AES. But symmetric-key cryptography has some limitations. One major limitation is the key distribution problem. If in case key, while sending through the channel, get compromised, whole communication will get vulnerable to attacks.

**PRIVATE KEY ENCRYPTION:**

It is also referred to as conventional encryption or single-key encryption, was the only type of encryption in use prior to the development of public key cryptosystem in the 1970s. In secret key cryptosystems, a single key is used for both encryption and decryption. As shown in Figure 5, the sender uses the key (or some set of rules) to encrypt the plaintext and sends the ciphertext to the receiver. c. With this form of cryptography, it is obvious that the key must be known to both the sender and the receiver; that, in fact, is the secret. The biggest difficulty with this approach, of course, is the distribution of the key.

**PUBLIC KEY ENCRYPTION:**

The development of public-key cryptography is the greatest and perhaps the only true revolution in the entire history of cryptography [10]. The concept of public key cryptography evolved from an attempt to attack the most difficult problem associated with conventional symmetric cryptosystems: the distribution of private keys and the lack of secrecy thereof. Public-key cryptography provides a radical departure from all that has gone before. For one thing, public-key algorithms are based on mathematical functions rather than on substitution and permutation. More important, public-key cryptography is asymmetric, involving the use of two separate keys, in contrast to symmetric encryption, which uses only one key. The use of two keys has profound consequences in the areas of confidentiality, key distribution, and authentication.

**FEASIBILITY STUDY:**

Hybrid encryption is a mode of encryption that merges two or more encryption systems. It incorporates a combination of asymmetric and symmetric encryption to benefit from the strengths of each form of encryption. These strengths are respectively defined as speed and security.

Hybrid encryption is considered a highly secure type of encryption as long as the public and private keys are fully secure. A hybrid encryption scheme is one that blends the convenience of an asymmetric encryption scheme with the effectiveness of a symmetric encryption scheme. Hybrid encryption is achieved through data transfer using unique session keys along with symmetrical encryption. Public key encryption is implemented for random symmetric key encryption. The recipient then uses the public key encryption method to decrypt the symmetric key. Once the symmetric key is recovered, it is then used to decrypt the message.

The combination of encryption methods has various advantages. One is that a connection channel is established between two users’ sets of equipment. Users then have the ability to communicate through hybrid encryption. Asymmetric encryption can slow down the encryption process, but with the simultaneous use of symmetric encryption, both forms of encryption are enhanced. The result is the added security of the transmittal process along with overall improved system performance (Janssen, n.d.).

The hybrid cryptosystem is itself a public-key system, who’s public and private keys are the same as in the key encapsulation scheme. In place of public key system we can use digital signature like message digesting function with symmetric key system to make hybrid crypto system. Note that for very long messages the bulk of the work in encryption/ decryption is done by the more efficient symmetric-key scheme, while the inefficient public-key scheme is used only to encrypt/decrypt a short key value. For example, to encrypt a message addressed to user-1 in a hybrid technique user-2 does the following (Elminaam, Kader & Hadhoud, 2010; Gupta1 & Parvinder, 2013).

* Obtains user-1 public key.
* Generates a fresh symmetric key.
* Encrypts the message using the symmetric key.
* Encrypt the symmetric key using user-1 public key. And send both of these

encryptions to user-1.

To decrypt this hybrid cipher text, user-1 does the following:

* User-1 uses her private key to decrypt the symmetric key.
* User-1 uses this symmetric key to decrypt the message.

**INNOVATIONS IN PROJECT**

Database having the hybrid performance feature is the typical task in today’s world. Even though highly sophisticated security systems designed to protect their physical and digital perimeters, the data may still be at risk for a data breach. Therefore, they need to begin thinking about what they need to do to protect their data from the hacker. In an approach, the database security is protecting the data against hackers and identified threats. In today’s world it is moving on the factor that depends on the other technology or with other organization which gives rise to the concept of ‘hybrid’ terminology. In order to keep the data secure and preventing from unauthorized use, it needs some of the technology that is called encryption technology. In this research work, the technology is Data-in-Motion level. The database is originated from different locations with different combination of the data base. In Data-in-Motion level, the data are retrieved or transit in secure manner from the database. The database security is to protect the data from data damage also, if the user does need the data, then the user should encrypt it for as long as possible. Hence it keeps the concept of further high end performance computing with hybrid data under transaction. The proposed system of the hybrid encryption technique is highly securing the Data-in-Rest and Data-inMotion used in various applications such as banking, insurance systems, core banking, and web based applications. So this method proposes a strong security using RSA and SHA-1 algorithm. The proposed research work has successfully implemented and tested with existing algorithm of DES, Blowfish and AES algorithms to enhance the database security. The performance of proposed research work improves the strong security to protect the data and it will yield good impact on the database fields. In future, these methods would use some other encryption mechanism. The author concludes that research would help the data base administrator and free their big concerns to protect their data. The algorithm has tried different ways in data base that yields good result compare to normal security level. This method gives a better result compared with normal database without security concept. Every method has its own procedure and conditions. In this research work, it is having slightly memory overhead. So, some new methods are proposed for solving above said issues. Forthcoming researchers can also try different algorithms. Future Enhancements The future enhancement of the proposed Hybrid Encryption method involves securing online transaction in a cloud environment, wired environment, wireless environment and virtual network environment. The proposed hybrid encryption technique is also helpful in Mobile Banking and E- Banking. In virtual environment, data can be shared at two levels, such as Internet and Intranet. The proposed research work is used for sharing the secure data from one to others within the organization of the web server or virtual server at cloud environment. In Local Area Network, the proposed hybrid encryption mechanism may be customized for transferring the sensitive data from work station to host based applications. In web based applications, the proposed mechanism enables the transfer of sensitive data from user to user, from user to server and from server to server which are located outside of the organization. In a cloud environment, more number of people are accessing the web server locally or globally to share the sensitive data. The proposed hybrid encryption technique is very helpful to enhance the security for web based transactions in future.

**TEAM MEMBER WISE DISTRIBUTION OF WORK**

**Yukti Goyal (Team Leader):**

My main field will be to do research on various cryptographic algorithms of both symmetric and asymmetric encryption and how they both can be used to make more optimized algorithm on the basis of speed and security which is hybrid encryption of public and private key cryptography.

**Shubham Shukla:**

Shubham will research on various shortcomings of symmetric and asymmetric algorithms like DES(Data Encryption Standard), Triple DES, Diffie-Hellman and many more and also how these shortcomings can be overcome by using hybrid encryption.

**Pradipta Sarkar:**

Pradipta will look after the performance evaluation of symmetric and asymmetric algorithms like DES(Data Encryption Standard), Triple DES, Diffie-Hellman and many more and compare them and thus deduce an optimized algorithm for hybrid encryption.

**Mirtunjay Gupta:**

He will be doing research on future scope of cryptography and modern cryptography techniques which cannot be exploited using brute force attacks.

**REFERENCES**

Elminaam, D.S.A., Kader, H.M.A. and Hadhoud, M.M. (2010), ‘Evaluating the performance of symmetric encryption algorithms’, *International Journal of Network Security*, Vol. 10, No. 3, pp. 213-219.

Gupta1, R.K. and Parvinder, S. (2013), ‘A new way to design and implementation of hybrid crypto system for security of the information in public network’, *International Journal of Emerging Technology and Advanced Engineering*, Vol. 3, No. 8, pp. 108-115.

Janssen, C. (n.d.), ‘Hybrid encryption’, available at http://www.techopedia.com/definition/1779/ hybrid-encryption (accessed 22 November 2014).

Kuppuswamy, P. and Al-Khalidi, S.Q.Y. (2012), ‘Implementation of Security through simple symmetric key algorithm based on modulo 37’, *International Journal of Computers & Technology*, Vol. 3, No. 2, pp. 335-338.

Kuppuswamy, P. and Chandrasekar, C. (2011), ‘Enrichment of security through cryptographic public key algorithm based on block cipher’, *Indian Journal of Computer Science and Engineering*, Vol. 2, No. 3, pp. 347-355.

Ramaraj, E., Karthikeyan, S. and Hemalatha, M. (2009), ‘A design of security protocol using hybrid encryption technique’, *International Journal of the Computer, the Internet and Management*, Vol. 17, No. 1, pp. 78-86.

Shaar, M., Saeb, M., Elmessiery, M. and Badawi, U. (2003), ‘A hybrid hiding encryption algorithm (HHEA) for data communication security’, *Proceedings of 2003 IEEE 46th Midwest Symposium on Circuits and Systems*, Cairo, Egypt, pp. 476-478.

Tat Wi, C. (2010), ‘Implementation of hybrid encryption method using Caesar cipher algorithm’, Unpublished master thesis, University Malaysia Pahang (UMP), Pahang, Malaysia.