# Secure Text Transfer Using Diffie-Hellman Key Exchange Algorithm

Mrs .Sumitra Samal[1], Anurag Diwan[2], Nogesh Verma[3]
*[1]Asst. Professor,CSE Dept.,[2] B.ECSE Dept., [3]CSE Dept.*
*SSIPMT, Raipur, Chhattisgarh*

***Abstract--*** Encryption is the technique of hiding private or sensitive information within something that appears to be nothing be a usual. If a person views that cipher text, he or she will have no idea that there is any secret information. What encryption essentially does is exploit human perception, human senses are not trained to look for files that have information inside of them. What this system does is, it lets user to send text as secrete message and gives a key or a password to lock the text, what this key does is, it encrypts the text, so that even if it is hacked by hacker it will not be able to read the text. Receiver will need the key to decrypt the hidden text. User then sends the key to the receiver and then he enters the key or password for decryption of text, he then presses decrypt key to get secret text from the sender. Diffie-Hellman key exchange offers the best of both as it uses public key techniques to allow the exchange of a private encryption key. By using this method, you can double ensure that your secret message is sent secretly without outside interference of hackers or crackers. If sender sends this cipher text in public others will not know what is it, and it will be received by receiver.

***Keywords-*** Key Exchange, Public Key, Encryption , Decryption .

## I. INTRODUCTION

- Cryptography is the area of constructing cryptographic systems. Cryptanalysis is the area of breaking cryptographic systems. Cryptography is a field of computer science and mathematics that focuses on techniques for secure communication between two parties. This is based on methods like encryption, decryption, signing, generating of pseudo random numbers, etc
- There are four ground principles of cryptography:-
  1. Confidentiality : Defines a set of rules that limits access or adds restriction on certain information.
  2. Data Integrity : Takes care of the consistency and accuracy of data during its entire life-cycle.
  3. Authentication : Confirms the truth of an attribute of a datum that is claimed to be true by some entity.
  4. Non-Repudiation : Ensures the inability of an author of a statement respect a piece of information to deny it.
- The Diffie-Hellmann key exchange[1-3] is a secure method for exchanging cryptographic keys. This method allows two parties which have no prior knowledge of each other to establish a shared, secret key, even over an insecure channel. The concept uses multiplicative group of integers modulo, which without knowledge of the private keys of any of the parties, would present a mathematically overwhelming task to a code breaker .

## II. VISUAL BASIC

Visual Basic is a third-generation event-driven programming language and integrated development environment from Microsoft for its Component Object Model programming model first released in 1991 and declared legacy during 2008. Microsoft intended Visual Basic [4] to be relatively easy to learn and use. C is a general-purpose, imperative computer programming language, supporting structured programming, lexical variable scope and recursion, while a static type system prevents many unintended operations. Criticisms levelled at Visual Basic editions prior to VB.NET include:

1. Versioning problems associated with various runtime DLLs, known as "DLL hell".
2. Poor support for object-oriented programming.
3. Can only create multi-threaded applications using ActiveX or DLL.
4. Variant types have a greater performance and storage "overhead" than strongly typed programming languages.
5. Dependency on complex and fragile Component Object Model (COM) Registry entries.

## III. ALGORITHM

The simplest and the original implementation of the protocol uses the multiplicative group of integers module $p$, where $p$ is prime, and $g$ is a primitive root modulo $p$. These two values are chosen in this way to ensure that the resulting shared secret can take on any value from 1 to $p$–1. Here is an example of the protocol, with non-secret values in blue, and secret values in **red** [5-7]

1. Alice & Bob publicly agree to use a modulus $p = 23$ and base $g = 5$ (which is a primitive root modulo 23).
2. Alice chooses a secret integer $a = 4$, then sends Bob $A = g^a \bmod p$
   - $A = 5^4 \bmod 23 = 4$
3. Bob chooses a secret integer $b = 3$, then sends Alice $B = g^b \bmod p$
   - $B = 5^3 \bmod 23 = 10$

4. Alice computes $s = B^C \bmod p$
   - $s = 10^4 \bmod 23 = 18$
5. Bob computes $s = A^b \bmod p$
   - $s = 4^3 \bmod 23 = 18$
6. Alice and Bob now share a secret (the number 18).

Both Alice and Bob have arrived at the same value s, because, under mod p,

$$A^b \bmod p = g^{ab} \bmod p = g^{ba} \bmod p = B^a \bmod p$$

More specifically,

$$(g^a \bmod p)^b \bmod p = (g^b \bmod p)^a \bmod p$$

Note that only $a$, $b$, and $(g^{ab} \bmod p = g^{ba} \bmod p)$ are kept secret. All the other values – $p$, $g$, $g^a \bmod p$, and $g^b \bmod p$ – are sent in the clear. Once Alice and Bob compute the shared secret they can use it as an encryption key, known only to them, for sending messages across the same open communications channel.

## IV. DESIGN

Diffe-Hellman is not an encryption mechanism as we regularly consider them, in that we don't commonly utilize DH to encrypt data. Rather, it is a strategy for secure exchange of the keys that encrypt data. DH performs this protected exchange by making a "shared secret" between two devices. The shared secret then encrypts the symmetric key for secure transmittal. The symmetric key is some of the time called a "Traffc Encryption Key" or "Data Encryption Dey". The procedure starts when every side of the correspondence generates a private key. Every side then produces an public key [8-9] , which is a derivative of the private key. The two systems then exchange their public keys. Every side of the correspondence now has its own private key and the other system's public key . By running the mathematical operation against your own private key and the other side's public key, you produce a value. At the point when the far off end runs the same operation against your public key and its own private key, that end also creates a value. The critical point is that the two qualities produced are indentical. They are the "shared secret" that can encrypt data between systems.

At this point, the Diffe-Hellman operation could be viewed as complete. The shared secret is, after all, a cryptographic key that could encrypt traffic. In any case, fulfillment as of right now is exceptionally uncommon, on the grounds that the shared secret is an uneven key by its mathematical nature, and all asymmetric key systems are inherently slow. On the of chance that the two sides are passing next to no movement, the mutual mystery may scramble real information. But any attempt at bulk traffic encryption requires a symmetric key system, for example, DES, Triple DES or Advanced Encryption Standard[10]. In most real uses of the DH protocol, the shared secret encrypts a symmetric key for one of the symmetric algorithms, then transmits it safely, and the inaccessible end decrypts it with the shared secret. Which side of the correspondence creates and transmits the symmetric key fluctuates. In any case, it is more regular for the initiator of the correspondence to be the one that transmits the key. I ought to additionally call attention to that some kind of arrangement ordinarily strikes choose the symmetric algorithms, the mode of the algorithms , hash functions , key lengths, refresh rates, and so on. That arrangement is taken care of by the application, and is not a piece of Diffe-Hellman, but it is obviously an important task, since both sides must support the same schemes for encryption for it to function. This additionally indicates why key-administration arranging is so vital – and why poor key administration so frequently prompts failure of systems. When secure exchange [11-12] of the symmetric key is finished, information encryption and secure communication can happen . Figure depicts data encrypted and decrypted on every end of the communication by the symmetric key. Changing the symmetric key for expanded security is straightforward as of right now. The longer the time a symmetric key is in use, the less demanding it is to perform a fruitful cryptanalytic attack against it. In this manner, changing keys frequent,

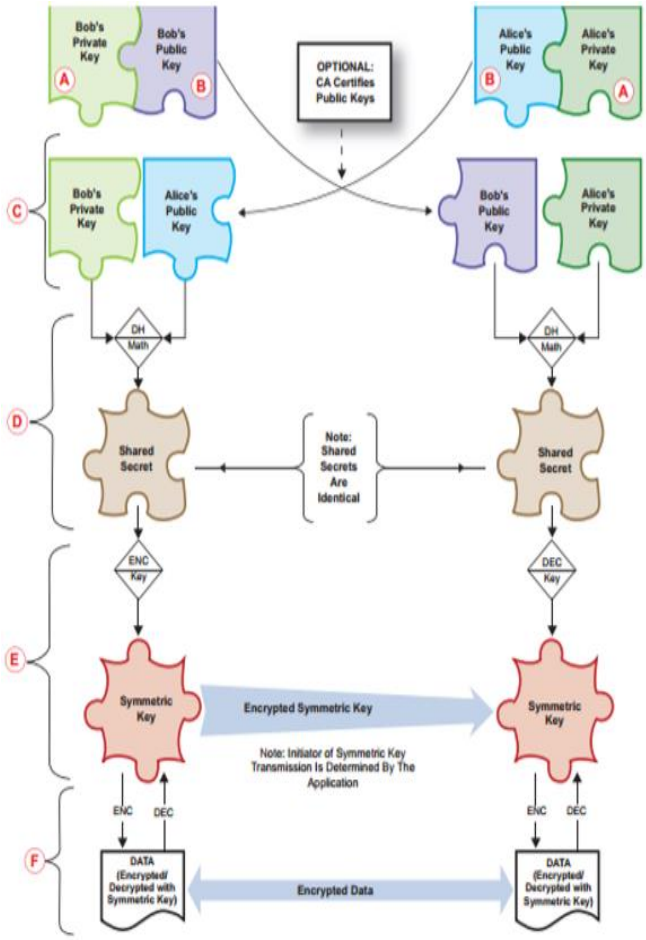



Fig.1: Diffie-Hellman Key Exchange

## V. METHODOLOGY

In order to improve the security performance of the text encryption algorithm, locations of pixels in the original text is shuffled and grey values of the shuffled text is changed. There is a class named form 1 in which there is a constructor to initialize all the components. We take a string type variable named hash in which we gave a key value. There are

functions for both button which do action on clicking. On clicking 1st button named encrypt the string of text box 1 is taken and converts it in the form of bytes by using UTF8 standard. Or UTF8 encoding. Then by using computehash we generate the key by using string of hash. Then by using Diffie-Hellman we create encryptor and encrypt the data of text box 1 by combining with key. Then change the encrypted result in the form of string and put it in text box 2. This is the encrypted string. Now on clicking the second button. Named decrypt. It takes the value of text box 2. Then convert it in form of bytes.

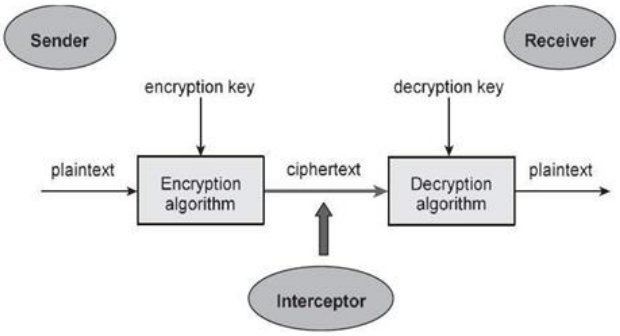



Fig.2: Block Diagram of Encryption & Decryption

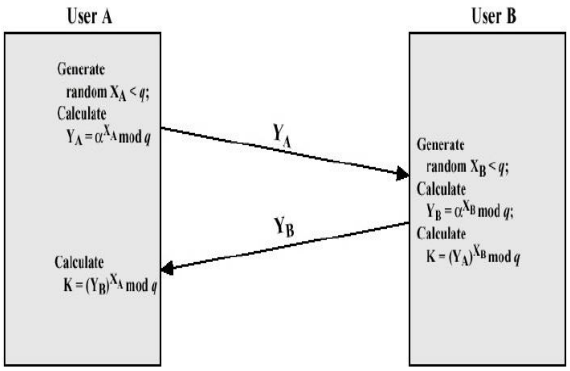
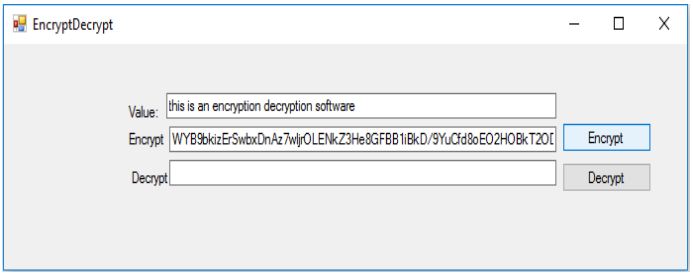



Fig.3: Diffie-Hellman Key Exchange

## VI. SCREENSHOTS



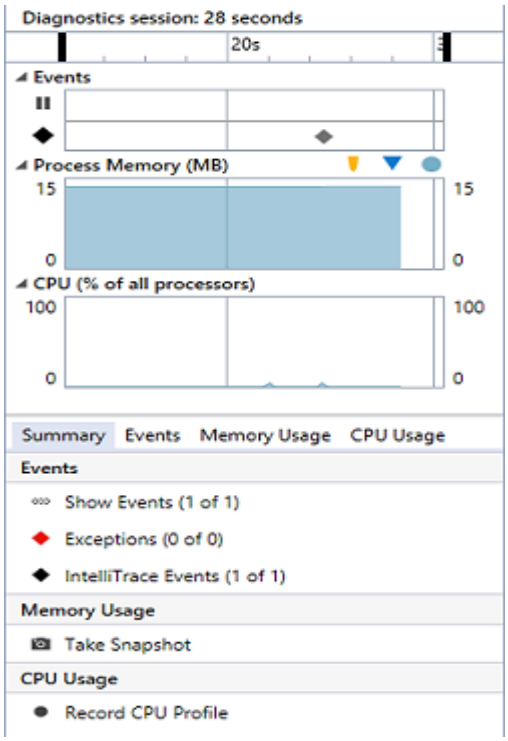




Fig.4: Result obtained after Encryption

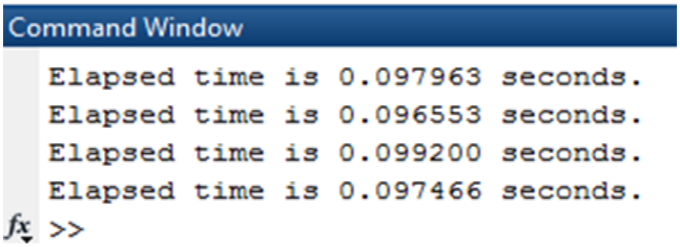
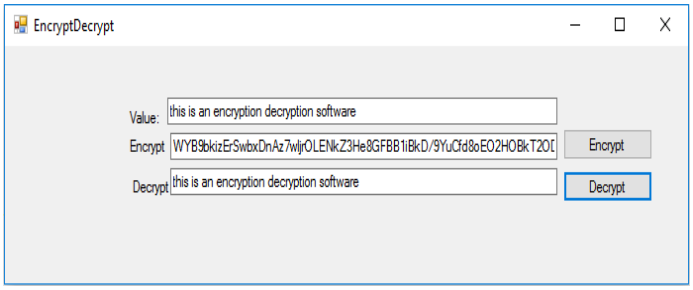



Fig.5: Time taken to Encrypt the message



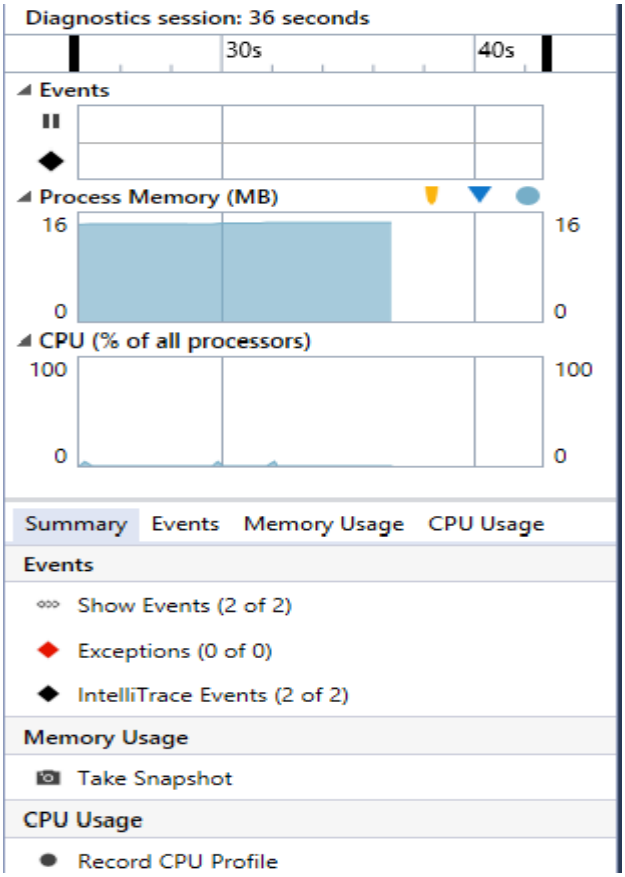



Fig.6: Result obtained after Decryption

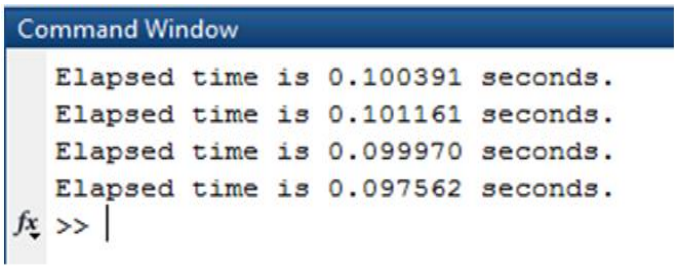



Fig.7: Time taken to Decrypt the message

## VII. ACKNOWLEDGEMENT

It is a great opportunity for us to express our profound gratitude towards our H.O.D, DR. JP Patra who gave us the motivation for making this project & whose zeal & enthusiasm are source of inspiration for us. Also, we can't ignore the innumerable efforts undertaken by Asst. Prof. Mrs. Sumitra Samal, our Project Guide, Department of Computer Science & Engineering, for her minute intricacies with constantly involving herself in our project devoting her valuable time. We would also like to thank all the staff members of Department of Computer Science & Engineering, Shri Shankaracharya Institute of Professional Management & Technology, Raipur(C.G), for their valuable assistance and support at all times.

## VIII. CONCLUSION

A new technique for text security using encryption and decryption by Diffie-Hellman is proposed. It is very easy to modify existing software to use Diffie-Hellman. It also has the advantage of Sharing of secret Key safely .The sender and receiver have no prior knowledge of each other . Communication can take place through an insecure channel .Uses secured SQL database to store the information.

## IX. REFERENCES

[1]. Philippe Refregier and Bahram Javidi Vol. 20, Issue 7, pp. 767-769 (1995) "Text encryption based on input plane and Fourier plane random encoding".

[2]. Guanrong ChenaYaobin Maob, Charles K. Chuic, "A symmetric text encryption scheme based on 3D chaotic cat maps".

[3]. Chaos-based text encryption algorithm Zhi-Hong Guana, Fangjun Huanga, Wenjie Guanb. A new text encryption algorithm based on hyper-chaos Tiegang Gaoa, Zengqiang Chenb.

[4]. Linhua Zhanga, b, Xiaofeng Liaoa, Xuebing Wangb "An text encryption approach based on chaotic maps".

[5]. Guohai Situ and Jingjuan Zhang "Multiple text encryption by wavelength multiplexing".

[6]. Shutian Liu, Quanlin Mi, and Banghe Zhu "Optical text encryption with multistage and multichannel fractional Fourier-domain filtering".

[7]. P.P. ; Dept. of Electr. & Comput. Eng., California Univ., San Diego, La Jolla, CA, USA ; Chau, P.M "Text encryption for secure Internet multimedia applications Dang,".

[8]. Rastislav Lukac, 1, , E-mail the corresponding author, Konstantinos N. Plataniotis, may 2005. "Bit-level based secret sharing for text encryption".

[9]. Henry Ker-Chang Chang,Jiang-Long Liu Graduate School of Resources Management, National Defense Management College, 1998. "A linear quadtree compression scheme for text encryption".

[10]. S.S. Maniccama, N.G. Bourbakisa AIIS Inc., 73100 Chania Crete, Greece b Wright State University, ITRI, College of Engineering and Computer Science, 3640 Glenn Hwy, Dayton, OH 45435, USA c TUC, ECE Department, 73100 Chania Crete, Greece February. 2004 "Text encryption using SCAN patterns".

[11]. http://cs.indstate.edu/~skallam/doc

[12]. https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange .