International Journal of Electronics Communication and Computer Engineering
Volume 3, Issue 1, ISSN 2249 –071X

# An Integrated Algorithm for Secured Communication with Digital Abstract Based on DES and Diffie Hellman

**Prashanna Gupta, Shweta Yadav**
prashanna_gupta@yahoo.co.in, shweta_yad@yahoo.co.in

***Abstract* - Security is the most promising field in networks and safe data transmission is a major task in this era. To enhance security in transmission different approaches have been developed but they are complex and useful for the small sized data. To improve the security level of data Transmission an integrated algorithm is proposed based on DES and Diffie Hellman with digital signature scheme SHA for providing digital abstract of the original data. This mechanism provides the confidentiality, completeness, Authentication and Integration. This paper presents the idea for securing the data transmission using the integrated algorithm useful for large sized data and also uses DES that provides the fast transmission. It is an effective algorithm to solve the problem of safe data transmission via internet.**

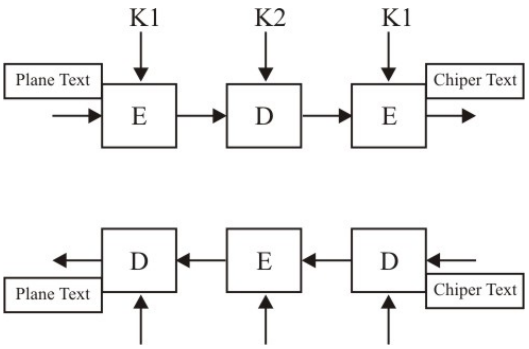
***Keywords:* - 3DES, Diffie Hellman key exchange, Digital Abstract, Secure Communication**

## I.INTRODUCTION

With the development of Internet, global information tide expends the application of information network technology. It also brings about great economical and social benefit along with the extensive use of this technology. However, because Internet is an open system which faces to public, it must confront many safe problems. The problems include network attack, hacker intruding, interception and tampering of network information which lead huge threat to Internet. Information security becomes a hot problem which is concerned by our society. This paper puts forward a safe mechanism of data transmission to tackle the security problem of information which is transmitted in Internet. The mechanism includes many properties that are confidentiality, completeness, authentication of identity, and non-repudiation. It bases triple DES algorithm and algorithm. Digital abstract algorithm MD5 is also included in this mechanism to protect the safe transmission of information.

## II.DES ALGORITHM

DES (Data Encryption Standard) algorithm is a traditional encryption technology. It developments in 20th century 70's and it was adopted by American government in November, 1976. Encryption and decryption of this algorithm are equivalence. The algorithm is open, but the key do not release. The security of System depends on the secrecy of the key. DES algorithm synthetically makes use of many cryptography technologies which include replacement, alternation and data input. It is a product cryptogram. Plaintext is divided into many blocks when encryption begins. Each block has 64 bits and the length of key is 64 bits. The valid length is 56 bits and the rest 8 bits are used for parity checking. First, 64 bits data is divided into two parts after initial replacement. Each part includes 32 bits. Then iterative process began. Right half 32 bits are extended to 48 bits. The result exclusive or with 48 bits sub-key which is got from 64 bits keys. The result is compressed as 32 bits through s box. After replacement, the 32 bits data exclusive or with left 32 bit data which is got from the beginning of replacement. Right half part of the new round is got. After 16 round replacements, a new 64 bits data is generated. There is one step we must pay attention to. The two results of last round do not exchange. The encryption and decryption can use the same algorithm through this process. To the last, the 64 bits result needs an inverse replacement. The 64 bits cipher text is got.




**STRUCTURE OF THE ENCRYPTION SYSTEM**

## III.DIFFIE HELLMAN KEY EXCHANGE

The Diffie Hellman key exchange algorithm solves the following dilemma. Alice and Bob want to share a secret key for use in a symmetric cipher, but their only means of communication is insecure. Every piece of information that they exchange is observed by their adversary Eve. How is it possible for Alice and Bob to share a key without making it available to Eve? At a first glance it appears that Alice and Bob face an impossible task. It was a brilliant insight of Diffie and Hellman that the difficulty

of the discrete logarithm problem for F*$p$ provides a possible solution. The first step is for Alice and Bob to agree on a large prime $p$ and a nonzero integer $g$ modulo $p$. Alice and Bob make the values of $p$ and $g$ public knowledge; for example, they might post the values on their web sites, so Eve knows them, too. For various reasons to be discussed later, it is best if they choose $g$ such that its order in F*$p$ is a large prime. The next step is for Alice to pick a secret integer $a$ that she does not reveal to anyone, while at the same time Bob picks an integer $b$ that he keeps secret. Bob and Alice use their secret integers to compute

$$A=g^a \pmod p \quad \text{and} \quad B= g^b \pmod p$$

They next exchange these computed values, Alice sends $A$ to Bob and Bob sends $B$ to Alice. Note that Eve gets to see the values of $A$ and $B$, since they are sent over the insecure communication channel. Finally, Bob and Alice again use their secret integers to compute

$$A' = B^a \pmod p \quad \text{and} \quad B' = A^b \pmod p$$

(Alice Compute this) (Bob Compute this)

The values that they compute, $\boldsymbol{A}'$ and $\boldsymbol{B}'$ respectively, are actually the same, since

$$A' = B^a = (g^b)^a = g^{ab} = (g^a)^b = A^b = B' \pmod p$$

The value exchange after the digital abstract computation and that digital abstract values are exchanged between the sender and receiver.

## IV. SHA-512

This Standard specifies five secure hash algorithms, SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512. All five of the algorithms are iterative, one-way hash functions that can process a message to produce a condensed representation called a *message digest*. These algorithms enable the determination of a message's integrity: any change to the message will, with a very high probability, result in a different message digest. This property is useful in the generation and verification of digital signatures and message authentication codes, and in the generation of random numbers or bits. Each algorithm can be described in two stages: preprocessing and hash computation. Preprocessing involves padding a message, parsing the padded message into $m$-bit blocks, and setting initialization values to be used in the hash computation. The hash computation generates a *message schedule* from the padded message and uses that schedule, along with functions, constants, and word operations to iteratively generate a series of hash values. The final hash value generated by the hash computation is used to determine the message digest SHA-512 may be used to hash a message, $M$, having a length of bits, where . The algorithm uses 1) a message schedule of eighty 64-bit words, 2) eight working variables of 64 bits each, and 3) a hash value of eight 64-bit words. The final result of SHA-512 is a 512-bit message digest. $0 \le \ell < 2^{128}$ The words of the message schedule are labeled $W^0$, $W^1$,…, $W^{79}$. The eight working variables are labeled ***a***, ***b***, ***c***, ***d***, ***e***, ***f***, ***g***, and ***h***. The words of the hash value are labeled $H^{(i)}, H_2^{(i)} \ldots\ldots H_7^{(i)}$, which will hold the initial hash value, $H^{(0)}$, replaced by each successive intermediate hash value (after each message block is processed), $H^{(i)}$, and ending with the final hash value, $H^{(N)}$. SHA-512 also uses two temporary words, $T1$ and $T2$.

## SHA-512 Pre-processing

1. Pad the message, $M$
2. Parse the padded message into $N$ 1024-bit message blocks, $M^{(1)}, M^{(2)} \ldots\ldots\ldots\ldots M^{(7)}$

Set the initial hash value, $H^{(0)}$

### SHA-512 Hash Computation

The SHA-512 hash computation uses functions and constants and Addition (+) is performed modulo $2^{64}$. After pre-processing is completed, each message block, $M^{(1)}$, $M^{(2)} \ldots\ldots\ldots\ldots M^{(N)}$ is processed in order using the following steps:

For i=1 to N:

{

1. Prepare the message schedule ,$\{W_t\}$

$$W_t = \begin{cases} M_t^{(i)} & 0 \le t \le 15 \\ \sigma_1^{\{512\}}(W_{t-2}) + W_{t-7} + \sigma_0^{\{512\}}(W_{t-15}) + W_{t-16} & 16 \le t \le 79 \end{cases}$$

2. Initialize the eight working variables, ***a***, ***b***, ***c***, ***d***, ***e***, ***f***, ***g***, and ***h***, with the (i-1)$^{st}$ hash value:

$A= H_0^{(i-1)}$, $B= H_1^{(i-2)}$, $C= H_2^{(i-2)}$, $D= H_3^{(i-3)}$, $E= H_4^{(i-4)}$, $F= H_5^{(i-5)}$, $G= H_6^{(i-6)}$, $H= H_7^{(i-7)}$

3. For $t$=0 to 79:

{

$T1= h + \sum_1^{\{512\}}(e) + ch(e,f,g) + K_t^{\{512\}} + W_t$

$T2= \sum_0^{\{512\}}(a) + Maj(a,b,c)$

$H= g$

$G= f$

$F= e$

$E= d + T_1$

$D= c$

$C= b$

$B= a$

$A= T_1 + T_2$

}

4. Compute the $i^{th}$ intermediate hash value $H^{(i)}$

{

$H_0^{(i)}=A+ H_0^{(i-1)}$
$H_1^{(i)}=B+ H_1^{(i-2)}$
$H_2^{(i)}=C+ H_2^{(i-2)}$
$H_3^{(i)}=D+ H_3^{(i-3)}$
$H_4^{(i)}=E+H_4^{(i-4)}$
$H_5^{(i)}=F+ H_5^{(i-5)}$
$H_6^{(i)}=G+ H_6^{(i-6)}$
$H_7^{(i)}=H+ H_7^{(i-7)}$

}

With the use of the above message digest algorithm find out the digital abstract of the data and then exchange between the sender and receiver.

## V. An Integrated Algorithm for Secured Transmission of Data Based on Triple Des and Diffie Hellman

**Sending Side:**

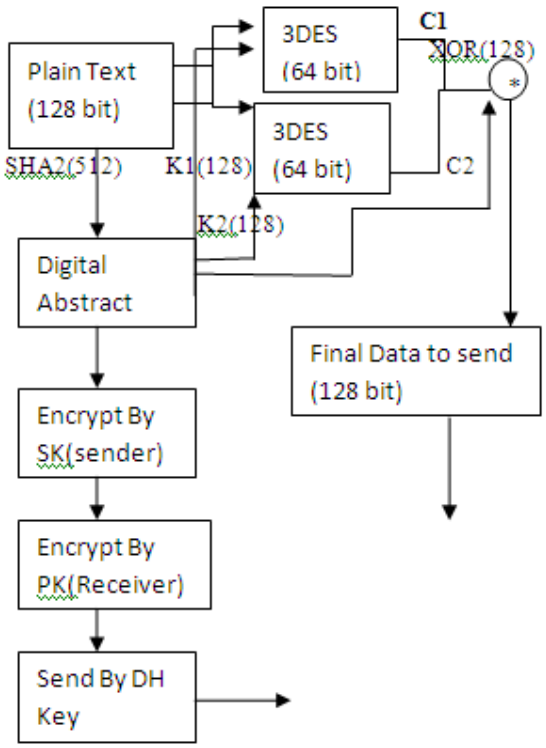
1. Calculate SHA2/512 of data
2. Divide the data into two 64 bit block
1. Encrypt the each block with triple DES. Select 128 bit of SHA2 as a Key for first block and select next 128 bit which will work as a Key for second bock.
3. After encryption combine the both block and take XOR with SHA2.
   (Choose predetermined 128 bit of SHA2/512 )
4. Encrypt SHA2/512 by Sender private Key and again encrypt by receiver public key.
5. Now exchange the Encrypted SHA2/512 by Deffie-Hellman
   (Exchange only once for any file)
6. Send only 128 bit Cipher text

**Receiving Side:**

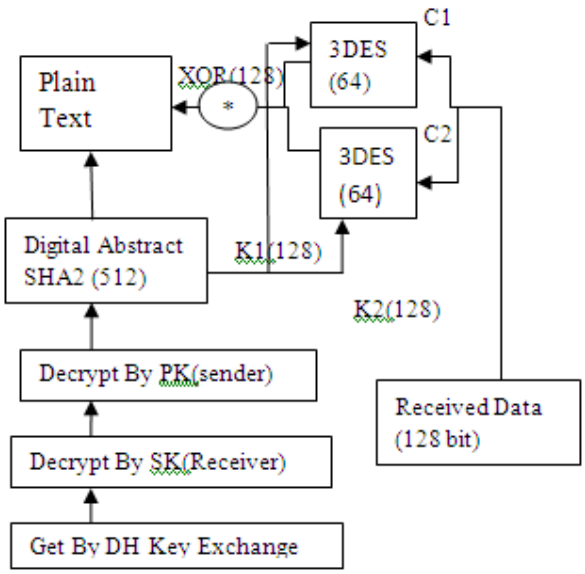
2. Get Encrypted SHA2/512 by Deffie-Hellman
   (Exchange only once for any file)
3. Decrypt by own private key and after that again decrypt by receiver public key.
4. Get SHA2/512
5. Divide the encrypted data into two 64 bit block
6. Decrypt the each block with triple DES. Select 128 bit of SHA2 as a Key for first block and select next 128 bit which will work as a Key for second bock.
7. After Decryption combine the both block and take XOR with SHA2.
   (Choose predetermined 128 bit of SHA2/512)
8. Get Plain Text

## VI. Model of The Approach

**Sending Side**




**Receiving Side**



## VII. ADVANTAGES & DISADVANTAGES

**1. Advantages**

First advantage of the system is that it provides the better functionality and super complexity.

Second advantage is that it is useful for the large data encryption and decryption.

Third is that it is more beneficial from the other system.

Fourth advantage is that it providing the best security mechanism.

Brute force Attack is not allowed in the system

**2. Disadvantage**

The major disadvantage of the system is that it is static in the nature and not provide any major key generation method so that when the key.

## VIII. CONCLUSION

An Integrated algorithm for secured communication based on Diffie Hellman and Triple DES provide greater efficiency for securing the data and also provide the fast transmission. It crate the digital abstract of the whole data that essencially verified by the receiver. This mechanism realizes the confidentiality, completeness, authentication and nonrepudiation. It is an effective method to resolve the problem of safe transmission in Internet.

## REFERENCES

[1] Kui-he yang, Shi-jin niu College of Information Hebei University of Science and Technology Shijiazhuang 050018, China "Data Safe Transmission Mechanism Based on Integrated Encryption," *Computational Intelligence and Software Engineering*, 2009.

[2] Wuling Ren College of Computer and Information Engineering Zhejiang Gongshang University *A Hybrid Encryption Algorithm Based on DES and RSA in Bluetooth Communication* Second *International Conference on Modeling, Simulation and Visualization Methods*, 2010.

[3] Yih Huang, David Rine, Xunhua Wang, "A JCA-based Implementation Framework for Threshold Cryptography," *Computer Security Applications Conference*, 2001.

[4] WUXing-Hui, ZHOU Yu-Ping, "Analysis of Data Encryption Algorithm Based on WEB," *2nd International Conference on Computer Engineering and Technology*, Volume 7, 2010.

[5] Othman 0. Khalifa, MD Rafiqul Islam', S. Khan' and Mohammed S. Shebani, "Communications Cryptography," *RF and Microwave Conference, October 5-6, Subang, Selangor, Malaysia*, 2004.

[6] Oracle Java cryptography architecture API specification & reference. Available at http://download.oracle.com/javase/6/docs/technotes/guides/security /crypto/CryptoSpec.html, 2011.

[7] Google Android Bluetooth APIs specification available at http://developer.android.com/guide/topics/wireless/bluetooth.html, November 2009.

[8] L. P. Zhao, L. B. Yang, "The usage of MD5 algorithm in RSA algorithm," Fujian Computer, vol 22, no. 4, pp. 63-64, May 2005.

[9] B. Jiang, "Synthesized encryption plan of DES and RSA," Micro-Computer Science, vol 23, no. 6, pp. 52-54, March 2006.

[10] S. P. Wang, Y. M. Wang, "Digital signature scheme based on DES and RSA," Journal of Software, vol 14, no. 1, pp. 146-150, June 2003.

## AUTHOR'S PROFILE

Name : Prashanna Gupta
Father : Mr. Dilip Kumar Gupta
Gander : Male
Date of Birth : 8th August 1986
Address : 131B Trade Center, South Tukoganj, Indore, MP, India
Email ID : prashanna.gupta@gmail.com
Contact No. : 91-9691230211
Graduation:
Degree : Bachelor of Engineering
Branch : Information Technology
College : Jawaharlal Institute of Technology, Borawan, MP, India
University : RGPV
Pass out : 2008
Teaching:
Designation : Lecturer
College : Central India Institute of Technology, Indore, MP, India
Post Graduation:
Degree : Master of Technology
Branch : Information Technology
College : Mahakal Institute of Technology, Ujjain, MP, India from University: RGPV
Research Area : Security
Research Work : An Integrated Algorithm for secured communication with digital Abstract based on DES and Diffie Hellman

Name : Shweta Yadav
Father : Shri Mahesh Yadav
Gander : Female
Date of Birth : 19 july 1979
Address: 419 LIG 2 ,90 Qr. Indira Nagar Ujjain
Email ID : shweta_yad@yahoo.co.in
Contact No .: 91-9329553757
Graduation:
Degree : Bachelor of Engineering
College : Hitkarni Collegeof Engg. Technology, Jabalpur, MP, India
University : RGPV
Teaching:
Designation : Reader
College : M.I.T.Ujjain
Post Graduation:
Degree : Master of Technology
Branch : Information Technology
College : Mahakal Institute of Technology, Ujjain, MP, India from University: RGPV
Research Work : Congestion Control through ECN Using RED algorithm
Research Area : Networking
5 publications : 3 of congestion control, 1 on VOIP, 1 on Signcryption, CSI memebership