INTERNATIONAL JOURNAL OF HIGHER EDUCATION AND RESEARCH
IJHER, Vol., 8(2), 2018, 322-333.
www.ijher.com

IJHER
(ISSN 2277 260X)

CODEN:IJHER ORIGINAL ARTICLE

SECURE AND AUTHENTICATED CRYPTOGRAPHIC TECHNIQUE

Vastvikta Pal[1], Sweta Srivastav[2], Vivek Kumar[3] and Kamal Kumar Gola[4]
[123]Department of Mathematics, Faculty of Engineering, TMU, Moradabad, 244001 India.
[4]Department of Computer Science and Engineering, Faculty of Engineering, TMU, Moradabad, 244001 India.
*Corresponding author Email: <vastvikta0691@gmail.com, kkgolaa1503@gmail.com>

ABSTRACT

This paper mainly focuses on the technique to secure our data in such a way that it provides confidentiality and authentication or verification both. Cryptography a well-known security technique used for securing a data. In daily life the importance of online transactions is rapidly increasing so is the rates to hack it and decode the message between two individuals are increasing. The rate of threats are increasing which are letting insecurities in people related to the data and which means that we need a system of network securities which not only provides verification of the message but also maintain the equilibrium that the message is not leaked to the third person or the hacker. PKC (public key cryptography) provides confidentiality while Digital signature provides authentication only. Thus, we designed a cryptography technique which not only provides authentication but the confidential data is also safe. In short it provides both the operations in a single algorithm; this is what we are working on.

INTRODUCTION

Nowadays the sharing of information is done electronically. Most of the data is in electronic form and it is very important to maintain our information to be secure. Security is the most stimulate elevation in the world of internet and network applications. There are various methods or techniques

to maintain our information to be secure but still some other factors that need to be considering like 1execution performance metric and cost of execution. Cryptography is one of the most important methods that convert the normal form of the message into the unreadable form of the message. The two main characteristics of cryptosystem that recognize and differentiate the message by encryption or decryption algorithm from another are its skill to secure the data against attacks and the second one its speed and efficiency in doing so.

TYPES OF SECURITY RISK

There are two types of security risks.

1. **Passive Risks :-**

In this bluff, if someone eavesdropping our information and the other person who is the attacker keeping an eye on our information then he will get our information. The main aim of the opponent is to get the information which is being transmitted from the system without affect the system resource. They are divided into two categories.

a) Leak of data information:-

A telephonic, e-mail conversation and a transferred file which consist a confidential data .We supposed to prevent our information from the hacker during the transmission of data.

b) Traffic Analysis:-

It is a kind of Risk which done on encrypted message. The hacker might be able to crack the code of such encrypted message. Also knows about the frequency, length of the data being exchanged and identify the location of the commutator.

2. Active Risks:-

It includes some alteration of the data or adding some false information. The main aim of this risk is to modify the system resource or affect their operation. They are divided into four categories.

a) Masquerade:-

It takes place when one stuff pretends to be a different stuff. For example the privileges are obtained by the stuff that has already the privilege and the authentication sequence is used after a valid authentication is already there.

b) Alteration of data information:-

It means that some portion of message is altered to produce an unconstitutional effect.

c) Contradiction of service:-

It blocked intentionally all the data to reach a particular destination by an attacker. Its target is to affect the network by overloading it with data so as to corrupt the performance.

d) Replay:-

It includes the passive grab of data and retransmission to produce it.

LITERATURE REVIEW

Dhawan [1] has discussed the different algorithms of encryption under the .NET. According to the author different algorithms were compared with others like DES, 3DES, RC2 and AES. This mainly concludes that AES is better in comparison to the other algorithms of cryptography.

B.Nithya and P.Sripriya[2] have discussed in this paper that presents a review of study of algorithms and their comparisons. Keywords used are plaintext, encryption, decryption, security attacks. The conclusion includes those different types of algorithms and their speed and memory and this shows that symmetric algorithm

Tamimi [3] has discussed in the research paper that the symmetric algorithms in which the comparison was made by the author were AES, DES, 3DES and Blowfish. This includes two modes of operation ECB, CBC this also includes C# programming language for working. It concludes that AES is poor in time management as compared to other algorithms are faster that asymmetric algorithms.

Mandal et al [4] have made a comparison between the most known symmetric algorithms DES, 3DES, AES and Blowfish. Comparison among these keys were made on the basis of the size, round block size, key, encryption/decryption time, and CPU process time and power consumption.AES is the best among all under this research paper while 3DES is the worst algorithm in all aspects.

Cornwell [5] discussed in the research paper about the cryptographic keys and it mainly focuses on the BLOWFISH algorithm and thus, he concluded that the BLOWFISH algorithm in comparison with the other algorithms DES,3DES,AES is better in many ways like the security of data BLOWFISH is more reliable than the other algorithms and is more effective in key size, security of data and etc. he designed the particular BLOWFISH algorithm for the encryption of data and thus its security purposes and attacks in cryptography techniques

Marwaha et al [6] discussed in the research paper about the three algorithms of the cryptography namely DES, 3DES, RSA. The DES and 3DES are symmetric algorithms which uses same key for encryption and decryption process “private” and “public” keys. While RSA algorithm is asymmetric key cryptography and uses different keys for encryption and decryption “public” or “private”. They

discussed in the research paper that the term security is valid and more useful for the3DES algorithm in comparison to the other algorithms DES and RSA. It was concluded in this research paper that which algorithm is more secure and valid for the different keys of encryption and decryption process. For hacking purposes the DES algorithm is very weak as it takes less time for the encryption and decryption of messages and thus is less secure in comparison to the other two algorithms 3DES and RSA

Saini [7] discussed in the research paper about the different algorithms and its performances comparison DES, AES, RC2, RC6, 3DES and BLOWFISH. He studied various research papers and tried to figure out that which algorithm is the best one. On the basis of table comparison and different studies on algorithms he compared different algorithms on the basis of the different keys, size, space, etc.

Abdul et al [8] discussed various algorithms of cryptography and their performances rate. They mainly discussed six algorithms AES, DES, 3DES, RC2, RC6 and BLOWFISH. These were compared so thus there performance rate were seen in the conclusion. They were compared on the parameter like key size, memory, security, shape, etc. their performances were noted and thus a very brief comparison was made between them their speed of encrypting and decrypting messages was also made and thus it was concluded that the BLOWFISH is the best performance algorithm in comparison to the other algorithms. The BLOWFISH algorithms followed by RC6 AND RC2 are good and more secure in comparison to the other algorithms. but these three algorithms have disadvantage over the other algorithms in terms of the time consuming power these algorithms were slow in comparison to AES,3DES,DES. They also concluded that 3DES is less secure in comparison to DES.

Seth et al [9] discussed in the research paper about the comparison of the algorithms mainly three algorithms were taken namely RSA, AES, DES. It was compared on the basis of their size, time,space and output results. He made various comparisons use different values and found that RSA uses more encryption time and its calculation was also very long and time taking it consumes more space and is less volatile than the other two algorithms. AES uses less space and DES is easy to calculate in comparison to the RSA algorithm. Deepti Chaudhary and Rashmi

Pallavi H. Dixit et al [10] discussed about the multilevel network security and steganography. This paper presents level security in network world. Cryptographic BLOWFISH algorithm and steganography algorithm LSB (list significant bit) for encrypting a message we use BLOWFISH and

then use LSB for hiding image. In this research paper the comparison on the basis of time, speed, and space was made and thus it is more beneficial for the embedded mobile security systems like ATM, mobile, online transactions, banking (online), smart card, visa, etc.

Proposed Algorithm

Key Generation at Sender's Side

Step 1 Firstly sender selects a prime number 'p'.

Step 2 Find the prime factor of (p-1) that means 'q' = (p-1).

Step 3 Now, Find the value of 'g' by the given equation, where g is the public key of sender

g = h^ (p-1/q) mod p, with the following conditions-

i) The value of 'h' is always less than (p-1) that means 'h' is less than (p-1) should be true.

ii) The value of h^ (p-1/ mod p) is always greater than 1 that means h^ (p-1/q) mod p is greater 1 should be true.

Step 4 Now, select the value of 'x' which is a private key of sender with condition that the value of 'x' is always less than q, where q is the prime factor of (p-1).

Step 5 Sender calculate the public key 'y' using the below equation: y = g^x mod p

Step 6 So, the public key for the sender are 'g', 'y', 'p', 'q' and private key 'x'.

Key Generation Process at Receiver's Side

Step 1 Find the value of 'x = p*q '.

Step 2 Now Calculate the value of ø (n) = (p-1)*(q-1).

Step 3 Calculate the receiver's public key by the given below equation: gcd (ø (n), e) = 1 with the following condition-

i) The value of 'e' will satisfy the condition 1<e< ø (n)

ii) 'e' should not be a factor of (p-1) and (q-1).

Step 4 Now, Calculate the private key'd' by the given below equation: (d*e) mod ø (n) = 1. Therefore, the receiver's public key is 'e' and private is'd'.

Singing Process

Step 1 Firstly, sender select a secret number 'k' for each message with condition 0 < k < q.

Step 2 Now, sender calculate the digital signature 'r','s' by using the given below equations:

r = (g^k mod p) mod q and s = [k^-1 (h (M) + x*r)] mod q where, M is the message to be signed and H (M) is the hash of message 'M'.

Encryption Process

Step 1 Finally, sender send the value of H(M) , 'r' , 's' which are encrypted by the receiver's public key to provide the confidentiality . So,

H (M)' = H (M) ^e mod n

r' = r^e mod n

s' = s^e mod n

Decryption Process

Step 1 Firstly, receiver decrypt all the values using own private key'd'

H (M) = [H (M)'] ^d mod n,

r = (r') ^d mod n

s = (s') ^d mod n

Step 2 After getting the value, receiver check the validity of signature that means the signature must verify the given conditions:

0 < r < q and,

0 < s < q

If digital signature fulfills the above conditions then, it will be accepted otherwise rejected.

Verifying Process

Step 1 Calculate the value of't' by the given below equation:

t = s^-1 mod q

V = [(g^H (M)) * y^r) ^t * mod p] mod q

If the value of V == r, then the signature is verified otherwise not.

Result Analysis

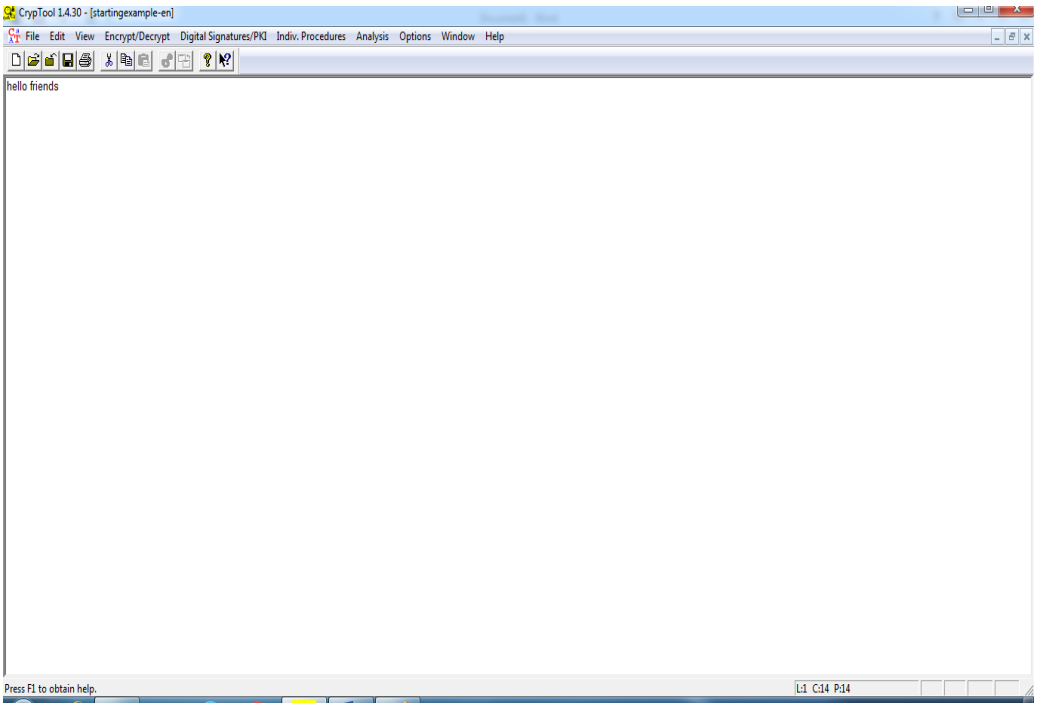

Fig 2. Input Message

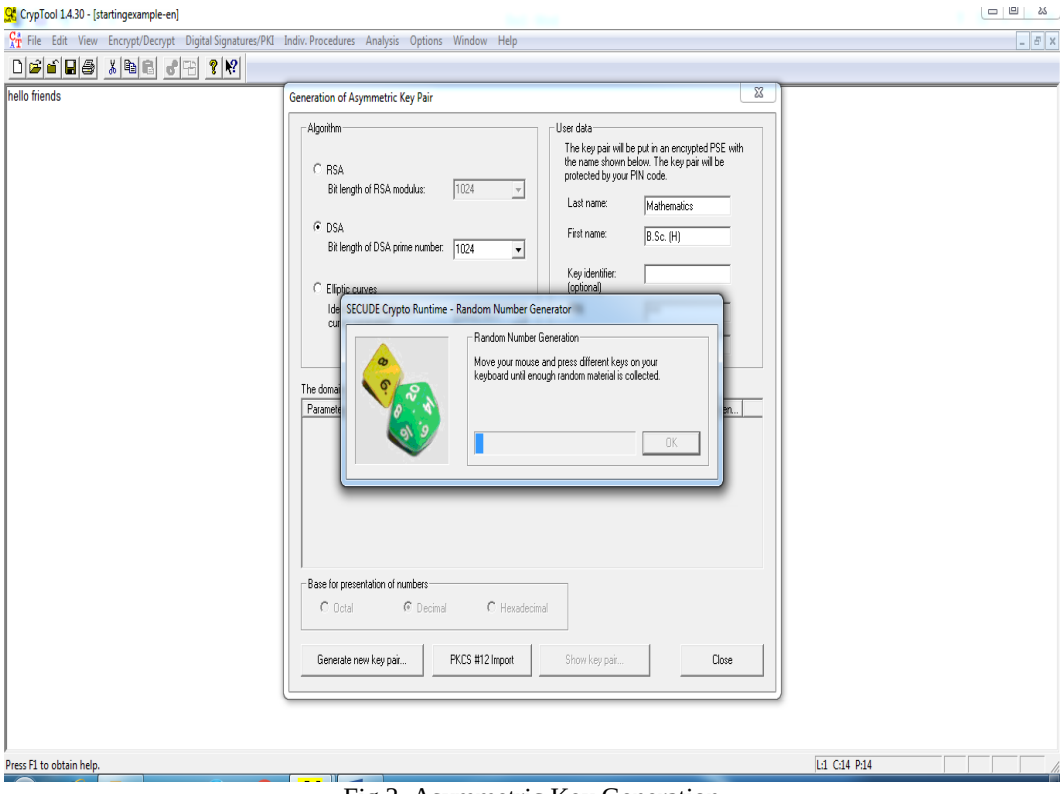

Fig 3. Asymmetric Key Generation

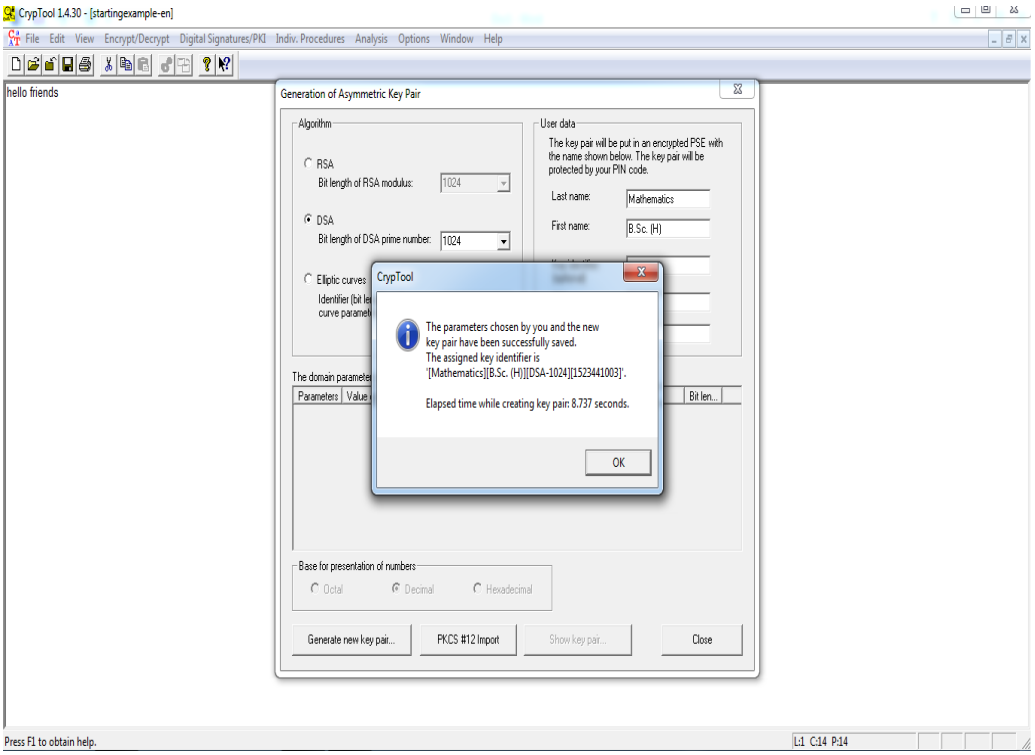

Fig 4. Parameters for Key Generation

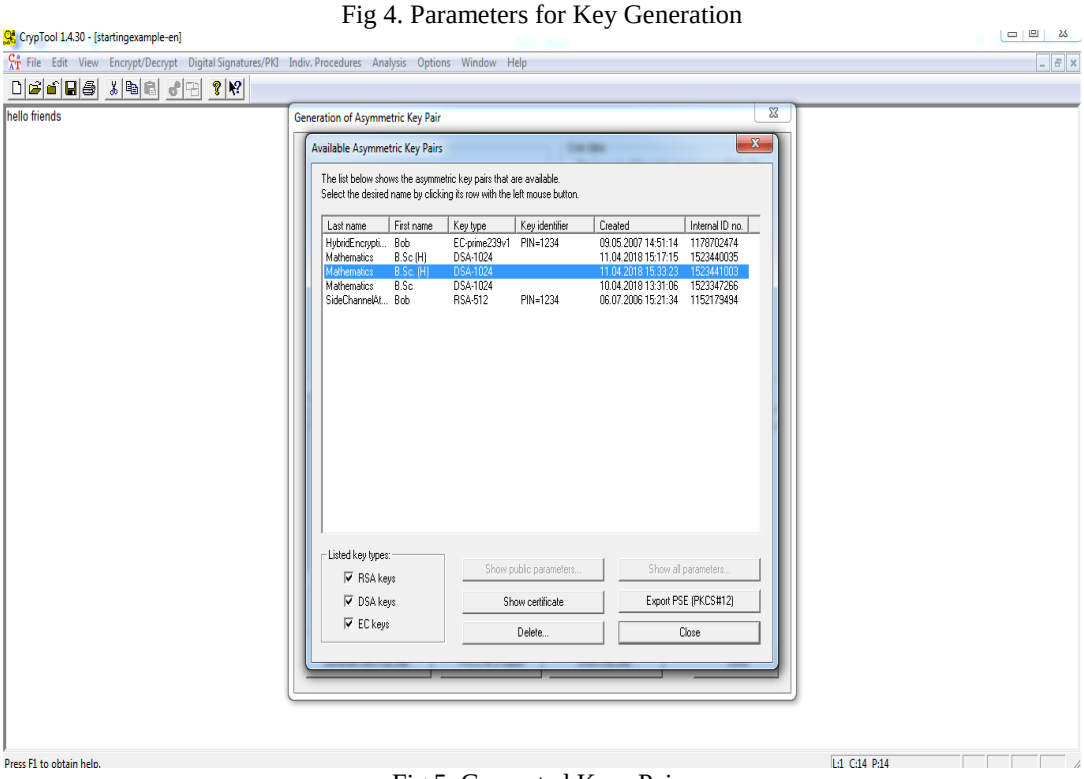

Fig 5. Generated Keys Pairs

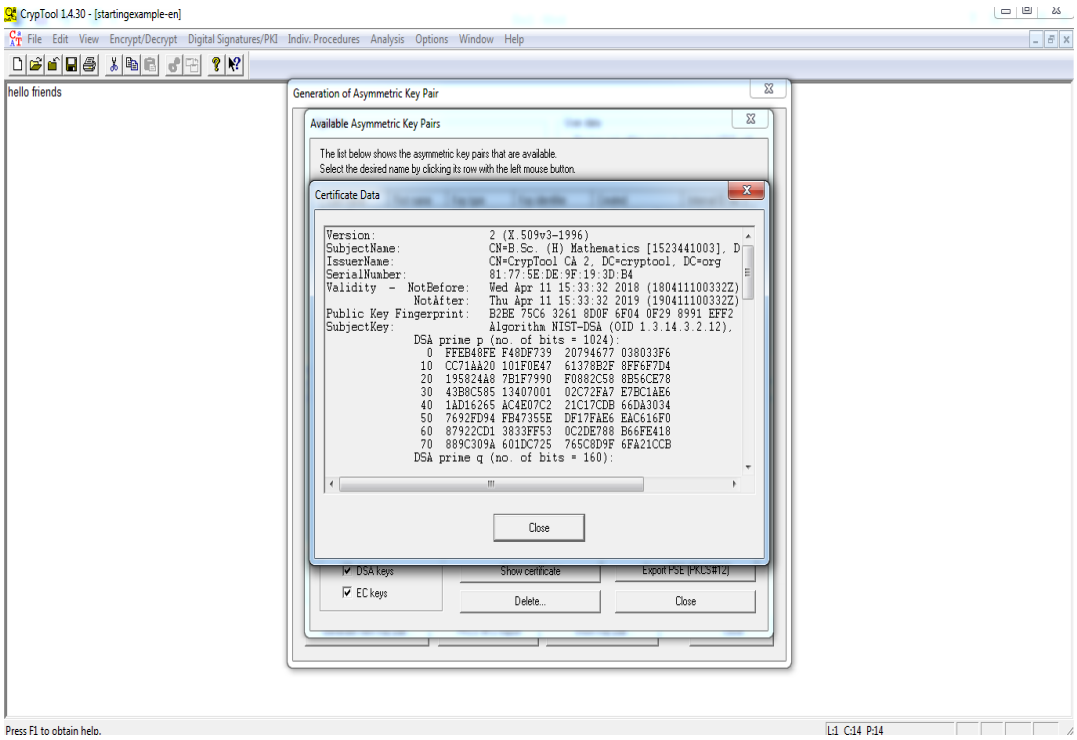

Fig 6. Certificate Data

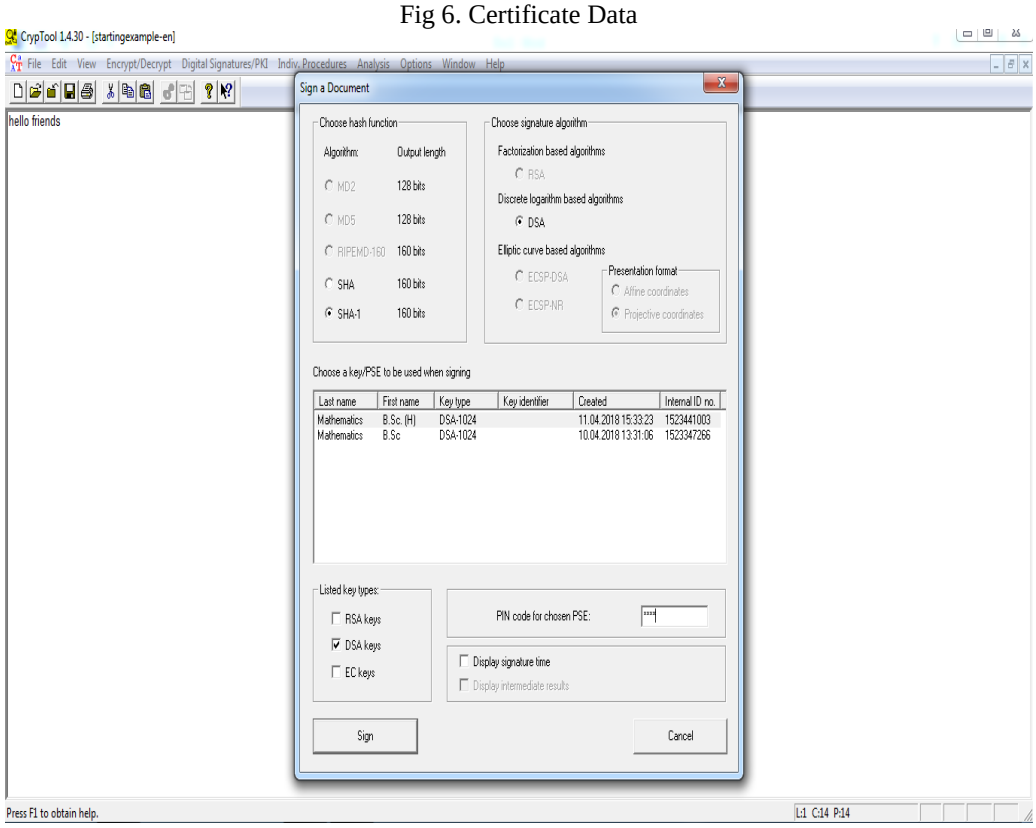

Fig 7. Sign Document

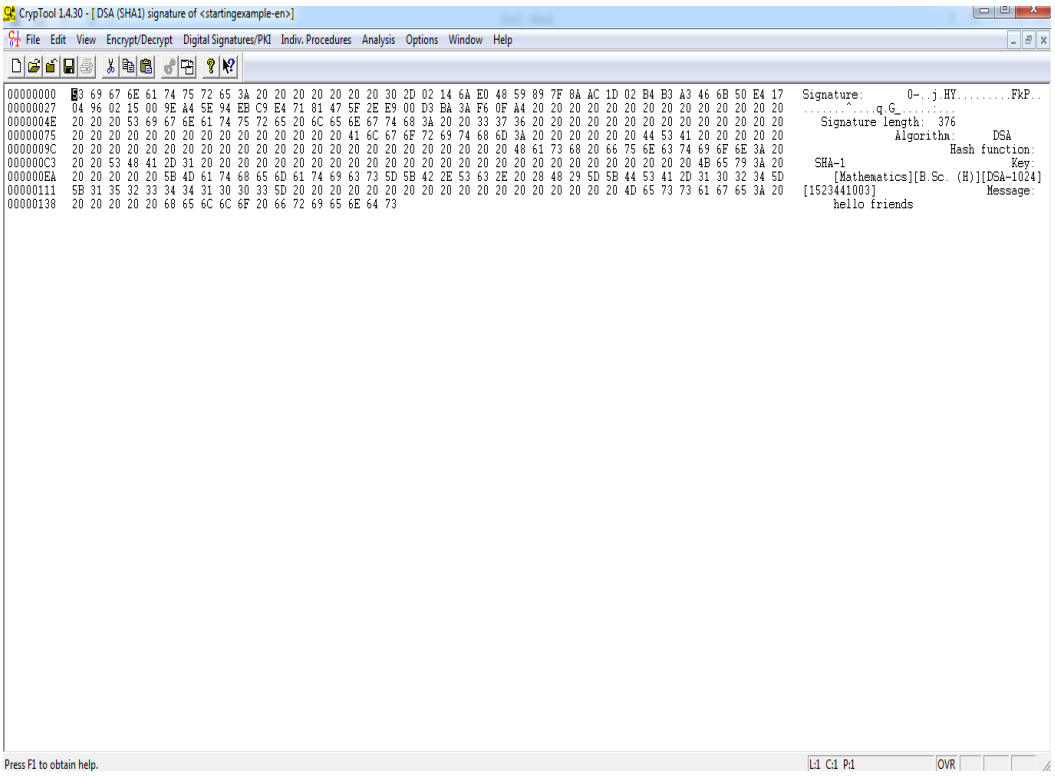

Fig 8. HEX Coding of Signed Document

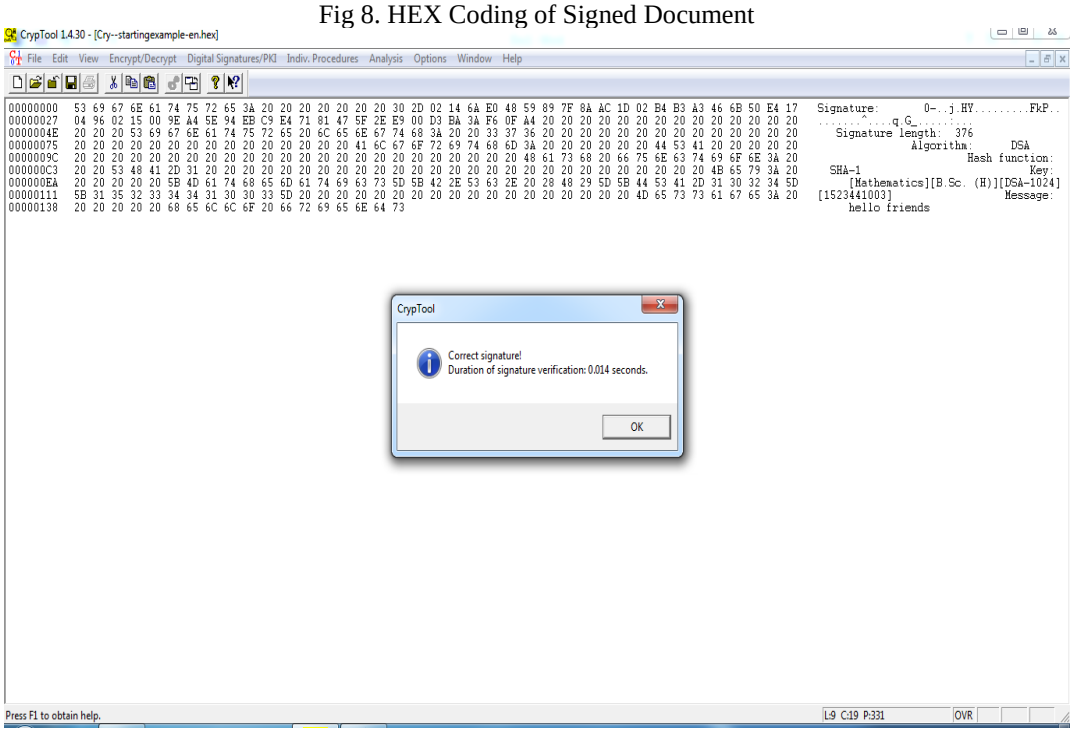

Fig 9. Signature Verification

CONCLUSION

In today's world, the protection of our data is very crucial thing because if anyone knows our data then they can misuse our data against anything. Therefore, Protection of Network Security is very important, without it our data can't be safe. In the world of Network Security, Cryptography is the most general method, to secure our data. In Cryptography, there are basically two types of method are used to achieve the confidentiality and the authentication. These two methods are Public Key Cryptography and Digital Signatures. Public Key Cryptography provides the confidentiality only as it uses a pair of key (i.e. public key and private key). While on the other hand, Digital signatures provides the authentication as it verifies the sender's signature. We can observe that our data should be either confidential or authenticated. And we want both (confidential and authenticated) at a same time. So we work on this issue, and proposed a new algorithm which gives both confidential and authentication at a same time.

REFERENCES

(1) Dhawan Priya, "Performance Comparison: Security Design Choices", Microsoft Developer Network October 2002.

(2) B.Nithya and P.Sripriya" A review of cryptographic algorithms in network security". International journal of engineering and technology (IJET). vol 8,no.1, FEB-MAR 2016. Pp - 324-331.

(3) Tamimi A. Al., "Performance Analysis of Data Encryption Algorithms", Oct 2008.

(4) Mandal Pratap Chandra, "Superiority of Blowfish Algorithm" IJARCSSE, volume 2, Issue 9, September 2012, pp. 196-201.

(5) Cornwell Jason W, "Blowfish survey", department of computer science, Columbus state university, Columbus, GA, 2010.

(6) MarwahaMohit, Bedi Rajeev, Singh Amritpal, Singh Tejinder, "comparative analysis of cryptographic algorithms", international journal of advanced engineering technology/IV/III/ July sep 2013/16-18.

(7) SainiBahar, "survey on performance analysis of various cryptographic algorithms", international journal of advanced research in computer science and software engineering, volume 4, issue 4, April 2014, pp-1-4.

(8) Abdul D.S, Kader H.M Abdul, Hadhoud, M.M., "Performance Evaluation of Symmetric Encryption Algorithms", Communications of the IBIMA, Volume 8, 2009, pp. 58- 64.

(9) Seth Shashi Mehrotra, Mishra Rajan, "Comparative analysis of Encryption algorithm for data communication", International Journal of Computer Science and Technology, vol. 2, Issue 2, June 2011, pp. 292-294.

(10) Pallavi H.Dixit ,Kamlesh B.Waskar ,Uttam L.Bombale, "multilevel network security combining cryptography and steganography on ARM platform", journal of embedded systems, 2015, vol 3, no. 1, pp-11-15.