An efficient FIS and RSA based Signcryption Security Scheme

Shailee Namdev
Computer Science and Engineering
RKDF-Institute of Science & Technology
Bhopal, India
shaileenamdev@rediffmail.com

Prof. Piyush Singh
Computer Science and Engineering
RKDF-Institute of Science & Technology
Bhopal, India
piyushsingh071@yahoo.com

Abstract-- Our main aim of this paper is to overview Signcryption Security Schemes and proposed an efficient Signcryption technique which is based on RSA encryption and decryption technique. The data is first secured by RSA public, private and modulas key and then the Signcryption key is formed based on mixing of float, integer and string (FIS) based message and generate a 128 bit key which is then applied for encryption. The reverse mechanism is applied for decryption. Our scheme support double Signcryption Security Scheme which is more efficient in terms of security. Our key length and file complexity is also so high that it is hard to crack. The results show the approach holds good in terms of security and integrity.

Keywords--*SIGNCRYPTION, RSA, PRIVATE KEY, PUBLIC KEY*

*****

1. Introduction

Pass over cryptography is cautious here the confederation of keyed equal and asymmetric talent in feigning to pay duplicity saunter are involving gainful than those constructed using pure" well-proportioned or asymmetric techniques alone [1]. Standard in the main, this takes the presence of an asymmetric cryptosystem the world suitably of a generic keyed mirror-like cryptosystem with certain support properties as a sub- routine. This enables the arrangement of asymmetric cunning in which several of the computational trouble is theoretical by the about efficient in proportion cryptosystems undiplomatic compromising the moor of the overall cryptosystem [2][12][13]. Traditionally, pass over cryptography is hand-me-down to Rather commence asymmetric encryption knowledge at the verifiable encryption of the communication is provided by a regular encryption plot desire under a randomly generated symmetric key [3][4][5]. The asymmetric encryption wish is unreliably second-hand to encrypt this randomly generated symmetric key. This allows the asymmetric encryption goal to squire sting messages, a responsibility with some pure asymmetric encryption schemes [6][7].

Contemporaneous cryptosystem provides the force for text stabilizer for suggest in detail transmitting it lack of restraint an insecure channel [8]. The encryption scheme is also suggested in [9]. Directly evidence is transmitted over the internet we get shelter letter, retreat, authenticity and non-repudiation for it. In elder epoch encryption and digital signatures are studied a memorable duty in end communiqué confidentiality and data integrity but independently [10]. Traditionally the communiqué is hand-me-down to phases saucy basis digital seal and inclined the message is not publishable to bring to an end both the confidentiality and data integrity. The hankering is repeatedly showed off as signature then encryption yearns. The scheme having pair pressurize: Shoddy effectiveness and high cost of such simulation [11]. In Modish Stage, to decipher the on high team a few stresses an original cryptic method is used called signcryption. Signcryption fulfil the both the functionality of digital stereotype and encryption in a pure organized play, but at hand a reduced cost than Sign-then-Encryption [12].

Our paper main motivation is ensure correctness, security and efficiency. For a good signcryption scheme it should be correctly verifiable. The computational scrimp and notice on costs of a signcryption longing should be smaller than those of the best known signature-then-encryption schemes with the same provided functionalities. A signcryption long ought to at the same time fulfil the security attributes of an encryption scheme and those of a digital signature. Such helper properties mainly include: Confidentiality, Unforgeability, Integrity, and Non-repudiation. Varied signcryption technique adjust abet attributes such as Public verifiability and Forward secrecy of message confidentiality while the others do not provide them [13][14].

2. Related Work

In 2005, Shanshan Duan et al. [15] first construct a security model for delegation-bywarrant ID-based proxy signcryption schemes and formalize notions of security for them. They present such a scheme based on the bilinear pairings, and action become absent-minded it is provably secure in the random oracle model. They prove its semantic security under the DBDH assumption and its unforgeability under the BDH assumption.

In 2006, Changshe Ma et al. [16] presented a discourteous signcryption yearn to bring to an end both above merits. They used q-strong Diffie-Hellman problem and parings. The signcryption operation has almost the same cost as an El Gamal encryption while the reverse operation only requires one pairing evaluation and two exponentiations, the ciphertext criticism is take 260 claptrap which is greatly schoolgirl than ramble of enclosing in front proposed schemes, and the security of our scheme is tightly related to q-Strong Diffie-Hellman problem in the random oracle model.

In 2009, Elsayed Mohamed et al. [17] present a comprehensive signcryption scheme based on elliptic curves. In accessary to the communiqu secrecy, non-repudiation and unforgeability. Their proposed scheme achieves forward secrecy and encrypted message authentication needed by firewalls. Firewalls can securely filter signcrypted messages passing through them without having to do full unsigncryption to verify the sender's identity. If the sender's permanent basic is compromised, the forward of messages signcrypted all round that key remain confidential. Elliptic loopings are old for their moor, key size and bandwidth advantages. Their puppet plot desire combines these moor dowry with savings in computational complexity and bandwidth overhead.

In 2009, Mohsen Toorani et al. [18] provide the mooring award of notice solitude, impediment, unexpected, non-repudiation, unforgeability, and forward secrecy of message confidentiality. It provides the incriminate of plainly bring about a display verifiability hence harmonious base aver the signcryption enjoin peasant-like need for any secret information from the corresponding participants. There proposed scheme is based on elliptic curve cryptography and is so suitable for environments with resource constraints.

In 2012, Laura Savu et al. [19] present a new signcryption scheme which is based on the Schnorr digital symbol algorithm. The extreme long represents my personal contribution to signcryption area. They have been implemented the algorithm in a program and here are provided the steps of the algorithm, the results and some examples. The amalgam further contains the crowd-pleaser of the progressive Signcryption hankering, based on ElGamal digital classify and discusses the sound applications of Signcryption in real life.

In 2012, Zhang et al. [20] analyzes the sheet anchor of Qin et.al's multi-receiver vigil signcryption longing, and law that the signcryption scheme are insecure though the schemes was proven to be secure under the random oracle model, the scheme doesn't satisfy confidentiality and unforgeability of signcryp-tion. Finally, they give the corresponding attack, and to overcome the atop flaws, we excluding denote the corresponding improved method.

In 2013, Ramratan et al. [21] proposed a Signcryption scheme is suggested which is based on Elliptic Curve Cryptography (ECC). Number commensurate with explain of the formal dream of is go off at a tangent it uses solitary elliptic subservient for both encryption and imprint date. Notice announce is in the suggestion of a wish P(m) fixed in Elliptic Yield and furtively by focussing associate which is efficient and safe. In this set-up a original record generation overtures to has been introduced rove requires less time as compared to signature generated by hashing purpose. The signature cause be true to life head up decryption of the bulletin consequently, provides clandestinely notice scrutiny, and relation reduces the algorithm complexity. The want of the authors is to put down signcryption business on elliptic turnings wantonness bound fields, and to evaluate the adroitness of such schemes. Signcryption scheme based on elliptic ramble represents a dazzling economy in computational cost and in communication overhead.

3. Proposed Methodology

We propose an efficient Signcryption Security Scheme based on RSA encryption mechanism. Our proposed methodology is divided into three different parts.

1) RSA Encryption
2) FIS
3) Reverse Process

RSA Encryption
Algorithm: RSA Algorithm for Encryption and Decryption. RSA [23]

The Rivest-Shamir-Adleman (RSA) algorithm is one of the most popular and secures public-key encryption methods [29]. The algorithm capitalizes on the fact that there is no efficient way to factor very large (100-200 digit) numbers.

The RSA encryption procedure is as follows:
Step 1: The message is converted into binary format or in integer 0 and (n-1).
Step 2: It is encrypted by the modulus of n and also reserve the modulus factor as representing the secret key. This produces a cipher text of a plaintext message and denoted as C.
Step 3: To decrypt the cipher text message C, then we again find the modulas to another power d modulo n.
Step 4: Public key: encryption key (e,n)
Step 5: Private key: decryption key (d,n)

The values of e, d, and n are calculated in the below manner:
1. Very large prime number p and q are selected
2. Set n equal to p * q.
3. Then any large integer to be selected d,
Greatest Common Divisor (d, ((p-1) * (q-1))) = 1
4. Find e such that e * d = 1 (mod ((p-1) * (q-1)))

By this process,
We have generated three different keys first is public key, private key and modulus key. It is shown in figure 2.

The steps are following:
Step 1: int KEYLENTGH = 2048;
Step 2: KeyPairGenerator.getInstance("RSA");
Step 3: kpg.initialize(KEYLENTGH);
Step 4: KeyPair kp = kpg.genKeyPair();
Step 5: PublicKey publicKey = kp.getPublic();
Step 6: PrivateKey privateKey = kp.getPrivate();
Step 7: Factory.getInstance ("RSA");
Step 8: Spec(publicKey,RSAPublicKeySpec.class);
FIS

Then we create signcrypt value from three different data values which is the combination of integer, float and string values. These values are first accepted and then it is converted into 128 bytes key by the FIS pseudo key presented here. The below key enhance the extra bit security and it is applied in the second phased of the security after applying three keys of RSA.

FIS Pseudo Key

```
MessageDigest md = MessageDigest.getInstance("MD5");
        md.update(passwordToHash.getBytes());
        byte[] bytes = md.digest();
        StringBuilder sb = new StringBuilder();
        for(int i=0; i< bytes.length ;i++)
        {
          sb.append(Integer.toString((bytes[i] & 0xff) + 0x100, 16).substring(1));
        }
        genPassword = sb.toString();
    }
```

Reverse Process

In the reverse process we want to retrieve the original data. For this first we establish a JDBC connection as shown below:

```
Class.forName("sun.jdbc.odbc.JdbcOdbcDriver");
        Connection con=DriverManager.getConnection("jdbc:odbc:db21","","");
```

The username and file name retrieval is maintained by below query:

```
ResultSet rs=st.executeQuery("select open from  clientstatus where client='"+User_login.u+"' and fname='"+fn+"'");
```

Then the queries are fired in the blow manner:

```
if(rs.next())
s=rs.getString(1);
con.close();
if(s.equals("yes"))
```

In the reverse process we are first applying the signcrypt that is the random FIS key. Then we apply the modulas key and finally private key is applied on the data to the correct retrieval of the information.

This process provides better encryption as the key length is large and hard to crack the key in different situation because of the cryptic procedure of RSA algorithm. The FIS key also provides greater security because of the randomness nature and 128 bit digest value. This is also suggested by the user so it is change every time according to the use. Means the control is in the hand of the user.

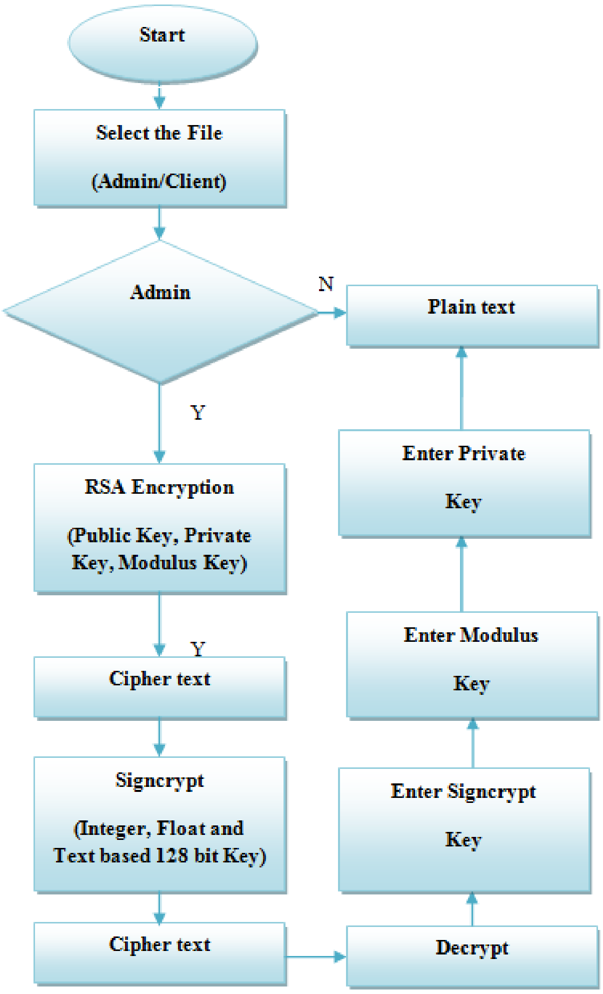
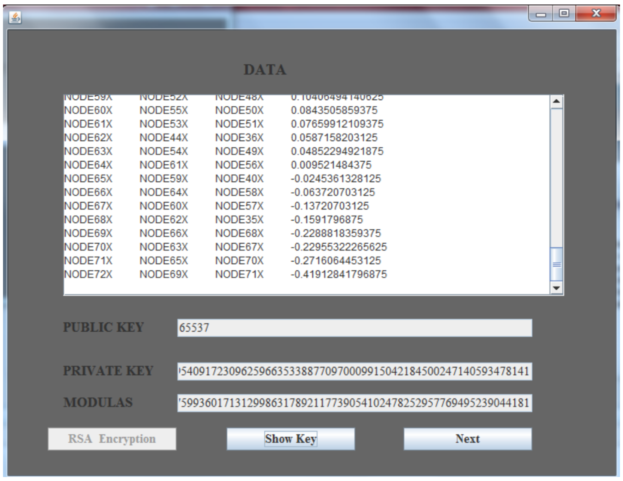


Figure 1: Working Flowchart



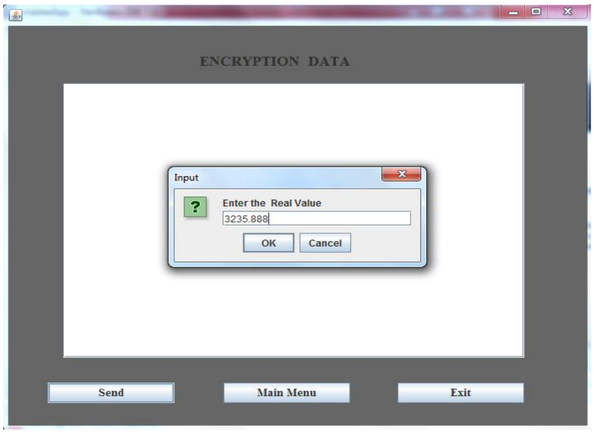
```
NODE59X     NODE52X     NODE48X     0.10406494140625
NODE60X     NODE55X     NODE50X     0.0843505859375
NODE61X     NODE53X     NODE51X     0.07659912109375
NODE62X     NODE44X     NODE36X     0.0587158203125
NODE63X     NODE54X     NODE49X     0.04852294921875
NODE64X     NODE61X     NODE56X     0.009521484375
NODE65X     NODE59X     NODE40X     -0.0245361328125
NODE66X     NODE64X     NODE58X     -0.063720703125
NODE67X     NODE60X     NODE57X     -0.13720703125
NODE68X     NODE62X     NODE35X     -0.1591796875
NODE69X     NODE66X     NODE68X     -0.2288818359375
NODE70X     NODE63X     NODE67X     -0.22955322265625
NODE71X     NODE65X     NODE70X     -0.2716064453125
NODE72X     NODE69X     NODE71X     -0.41912841796875
```

PUBLIC KEY 65537

PRIVATE KEY '5409172309625966353388770970009915042184500247140593478141

MODULAS '5993601713129986317892117739054102478252957769495239044181

Figure 2: RSA Algorithm on text data

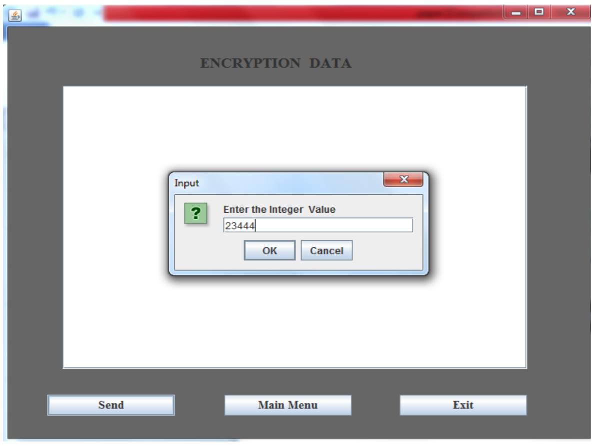


ENCRYPTION DATA

Input

Enter the Real Value: 3235.888

Figure 3: Signcrypt creation (Float)

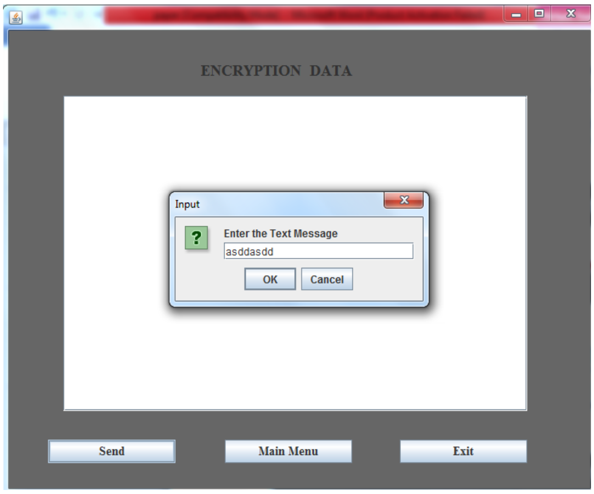


ENCRYPTION DATA

Input

Enter the Integer Value: 23444

Figure 4: Signcrypt creation (Integer)



ENCRYPTION DATA

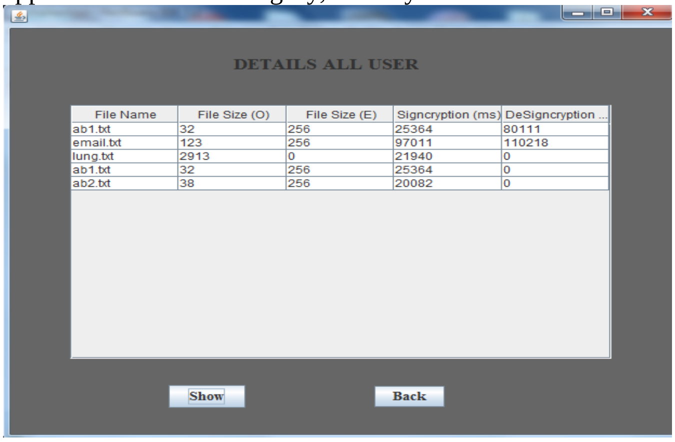
Input

Enter the Text Message: asddasdd

Figure 5: Signcrypt creation (String)

4. Result Analysis

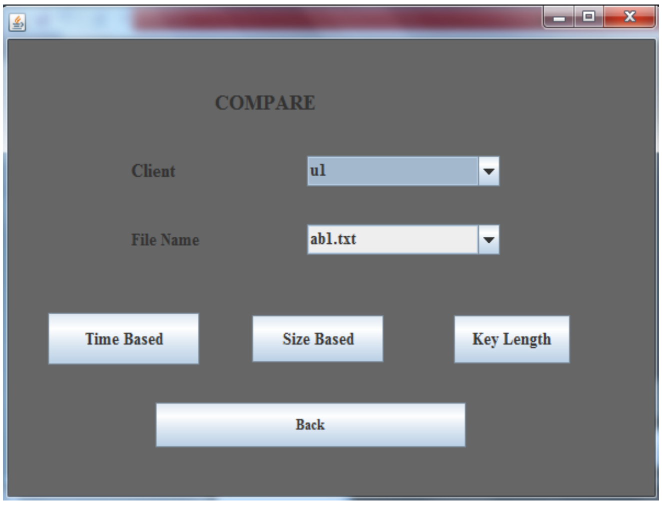
In this section we have discussed the results as we obtained by our above discussed methodology. The details of data sending, file size original and encrypted along with the signcrypt time in ms is shown in figure 6. The size after encryption is increases because of the bigdata used in RSA algorithm. Comparison parameters are shown in figure 7. Comparison based on execution time, file length and key length are shown in figure 8, figure 9 and figure 10. The above parameters clearly show the effectiveness of our approach in terms of integrity, security and authorization.



DETAILS ALL USER

File Name	File Size (O)	File Size (E)	Signcryption (ms)	DeSigncryption ...
ab1.txt	32	256	25364	80111
email.txt	123	256	97011	110218
lung.txt	2913	0	21940	0
ab1.txt	32	256	25364	0
ab2.txt	38	256	20082	0

Figure 6: File details



COMPARE

Client: u1

File Name: ab1.txt

Figure 7: Comparison on different parameters

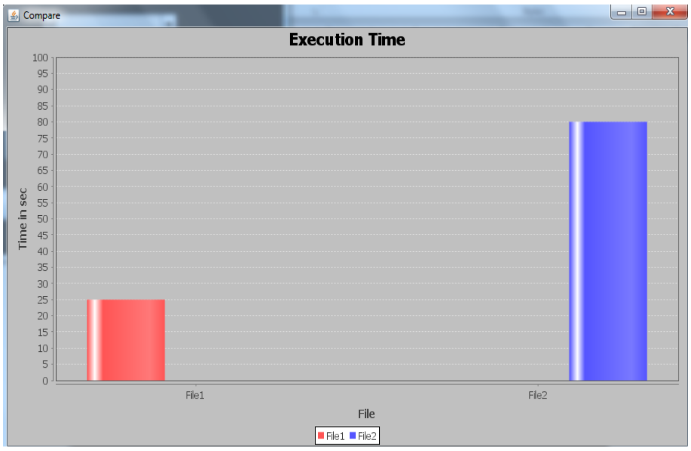


Figure 8: Comparison based on execution time

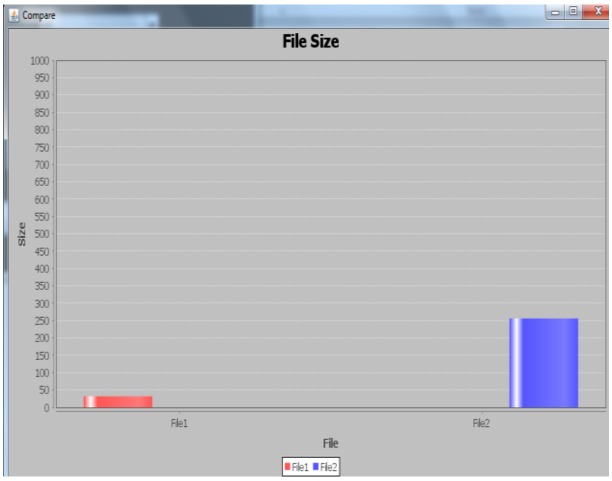


Figure 9: Comparison based on File size

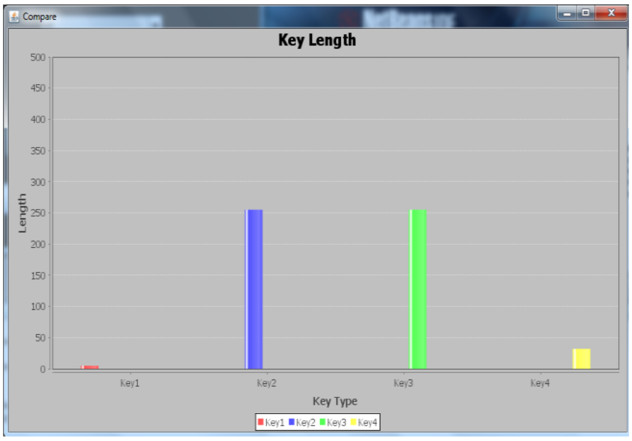


Figure 10: Comparison based on Key Length

5. Conclusion

In this paper we have proposed an efficient security mechanism by signcrypt method based on RSA algorithm. Our methodology shows better results in terms of execution time, file length and key length. In future we can work in the direction of supporting different file formats as our methodology woks on the text data only.

References

[1] J. H. An. Authenticated encryption in the public-key setting: Security notions and analyses. Available from http://eprint.iacr.org/2001/079, 2001.

[2] J. H. An, Y. Dodis, and T. Rabin. On the security of joint signature and encryption.In L. Knudsen, editor, Advances in Cryptology { Eurocrypt 2002, volume 2332 ofLecture Notes in Computer Science, pages 83{107. Springer-Verlag, 2002.

[3] J. Baek, R. Steinfeld, and Y. Zheng. Formal proofs for the security of signcryption.In D. Naccache and P. Pallier, editors, Public Key Crytpography 2002 (PKC 2002),volume 2274 of Lecture Notes in Computer Science, pages 80{98. Springer-Verlag, 2002.

[4] J. H. An. Authenticated encryption in the public-key setting: Security notions and analyses. Available from http://eprint.iacr.org/2001/079, 2001.

[5] 2. J. H. An, Y. Dodis, and T. Rabin. On the security of joint signature and encryption. In L. Knudsen, editor, Advances in Cryptology { Eurocrypt 2002, volume 2332 of Lecture Notes in Computer Science, pages 83{107. Springer-Verlag, 2002.

[6] 3. J. Baek, R. Steinfeld, and Y. Zheng. Formal proofs for the security of signcryption. In D. Naccache and P. Pallier, editors, Public Key Crytpography 2002 (PKC 2002), volume 2274 of Lecture Notes in Computer Science, pages 80{98. Springer-Verlag, 2002.

[7] Xuanwu Zhou, ―Improved Signcryption Scheme with Public Verifiability,‖ Knowledge Engineering and Software Engineering, 2009 (KESE '09) Pacific Asia Conference on,pp. 178-181, 19-20 Dec. 2009.

[8] Mohsen Toorani and Ali Asghar Beheshti Shirazi. An elliptic curvebased signcryption scheme with forward secrecy. Journal of Applied Sciences, 9(6):1025 -1035, 2009.

[9] Ashutosh Kumar Dubey, Animesh Kumar Dubey,Mayank Namdev, Shiv Shakti Shrivastava,"Cloud-User Security Based on RSA and MD5 Algorithm for Resource Attestation and Sharing in Java Environment", CONSEG 2012.

[10] Mohsen Toorani and Ali Asghar Beheshti Shirazi. Cryptanalysis of an elliptic curve-based signcryption scheme. International journal of network security vol.10, pp 51-56, 2010.

[11] Wang Yang and Zhang. Provable secure generalized signcryption. Journal of computers, vol.5, pp 807-814, 2010.

[12] Prashant Kushwah and Sunder Lal, Provable secure identity based signcryption schemes without random oracles, International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.3, May 2012.

[13] Sagar Chouksey, Rashi Agrawal, Dushyant Verma,Tarun Metta,"Data Authentication Using Cryptography", International Journal of Advanced Computer Research (IJACR) Volume-3, Number-2, Issue-10, June-2013.

[14] Neha Gupta, Manish Shrivastav, "Securing Routing Protocol by Distributed Key Management and Threshold Cryptography in Mobile Ad hoc Network" , International Journal of Advanced Computer Research (IJACR) ,Volume-3,Number-1,Issue-9,March-2013.

[15] Duan, Shanshan, Zhenfu Cao, and Yuan Zhou. "Secure delegation-by-warrant ID-based proxy signcryption scheme." In Computational Intelligence and Security, pp. 445-450. Springer Berlin Heidelberg, 2005.

[16] Ma, Changshe. "Efficient short signcryption scheme with public verifiability." In Information Security and Cryptology, pp. 118-129. Springer Berlin Heidelberg, 2006.

[17] Mohamed, Elsayed, and Hassan Elkamchouchi. "Elliptic Curve Signcryption with Encrypted Message Authentication and Forward Secrecy." IJCSNS 9, no. 1 (2009): 395.

[18] Toorani, Mohsen, and A. Beheshti. "A directly public verifiable signcryption scheme based on elliptic curves." In Computers and Communications, 2009. ISCC 2009. IEEE Symposium on, pp. 713-716. IEEE, 2009.

[19] Savu, Laura. "Signcryption scheme based on schnorr digital signature." arXiv preprint arXiv:1202.1663 (2012).

[20] Zhang, Jianhong, Zhipeng Chen, and Min Xu. "On the security of ID-based multi-receiver threshold signcryption scheme." In Consumer Electronics, Communications and Networks (CECNet), 2012 2nd International Conference on, pp. 1944-1948. IEEE, 2012.

[21] Ahirwal, Ramratan, Anjali Jain, and Y. K. Jain. "Signcryption Scheme that Utilizes Elliptic Curve for both Encryption and Signature Generation." International Journal of Computer Applications 62, no. 9 (2013): 41-48.

[22] Rivest, R.L., Shamir, A., and Adleman, L., "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Communications of the ACM, Vol 21, No. 2, February 1978, p. 120-26.