HYBRID ENCRYPTION ALGORITHM BASED IMPROVED RSA AND DIFFIE-HELLMAN

Miss. Renushree Bodkhe*

Prof. Vimla Jethani*

Abstract

Internet and Network applications have seen a tremendous growth in the last decade. As a result incidents of cyber attacks and compromised security are increasing. This requires more focus on strengthening and securing our communication. One way to achieve this is cryptography. Although a lot of work has been done in this area but this problem still has scope of improvement. In this paper we have focused on asymmetric key cryptography. In asymmetric key cryptography, also called Public Key cryptography, two different keys (which form a key pair) are used. One key is used for encryption & only the other corresponding key must be used for decryption. No other key can decrypt the message, not even the original (i.e. the first) key used for encryption. The beauty of this scheme is that every communicating party needs just a key pair for communicating with any number of other communicating parties. Once someone obtains a key pair, he /she can communicate with anyone else. RSA is a well known public key cryptography algorithm. It is the first algorithm known to be suitable for signing as well as encryption, and was one of the first great advances in public key cryptography. The security of the RSA cryptosystem is based on two mathematical problems: the problem of factoring large numbers know mathematical attack and the problem of trying all possible private keys know brute force attack. So to improve the security, this scheme presents a new cryptography algorithm based on novel method by combining the two most popular algorithms RSA as Improved RSA (IRSA) and Diffie-Hellman in order to achieve more security.

Keywords: IRSA, Cryptography, DH, Encryption, Decryption, etc.

* Ramrao Adik Institute of Technology, Nerul, Navi Mumbai

1. Introduction

One of the most important techniques to secure communication in the presence of third party is cryptography. Cryptography is the science which uses mathematics to encrypt and decrypt data. This science enables you to store sensitive information or transmit it across insecure networks so that it cannot be read by anyone except the intended recipient. In conventional cryptography, also called secret-key or symmetric-key encryption, one key is used both for encryption and decryption. In asymmetric cryptography, the encryption and decryption keys are different on both the sides. Hybrid cryptography is a combination of both symmetric and asymmetric cryptographic techniques. Hybrid cryptography is very effective indeed in providing high degree of security because whatever the problems associated with symmetric-key cryptographic techniques were solved when asymmetric cryptographic mechanism is used.Encryption is one of the principal means to grantee the security of sensitive information. It not only provides the mechanisms in information confidentiality, but also functioned with digital signature, authentication, secret sub-keeping, system security and etc.

Encryption is the process of conversion of data (called plain text) into an unreadable form (called a cipher text), this cipher text cannot be easily understood by unauthorized people. Decryption is the process of converting encrypted data back into its original form, so that it can be understood by the people who are authorized to read that data [3]. There exist many encryption algorithms that are widely used for information security. They can be categorized into symmetric (private) and asymmetric (public) key encryption. In practice, in order toachieve the optimal efficiency, the symmetric keyalgorithms and public key cryptography algorithms aregenerally combined together. Also Public-key cryptography can be used with secret-key cryptography to get the best of both worlds. Thus in this paper we have proposed a hybrid cryptographic algorithms by a combination of improved RSA and Diffie-Hellman. This combined approach is intended to get security advantage of public key system and speed advantage of secret key system.

1.1 Asymmetric Cryptography

In Asymmetric cryptography a pair of keys is used to encrypt and decrypt a message so that it is transmitted securely. Initially, a network user receives a public and private key pair from a Certificate Authority. The process of encryption using asymmetric cryptography can be explained by following steps -

- Use a key (public key) to encrypt a message.
- Another (private key) to decrypt a message.
- Private Key known to owner and used only by owner.

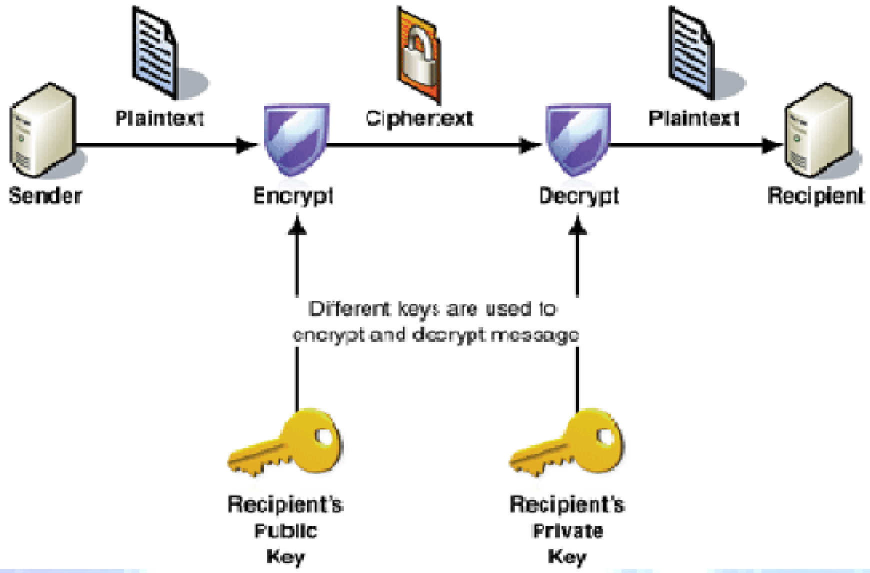

Figure 1: Asymmetric Key Encryption [7]

The advantage of using asymmetric key encryption is that it provides better key distribution and scalability in comparison of symmetric systems. RSA, Elliptic Curve Cryptosystem (ECC), Diffie-Hellman, El Gamal, Digital Signature Algorithm (DSA), Knapsack are some of the standard Asymmetric Key Algorithms.

1.2 RSA Algorithm

At present, the best known and most widely used public key system is RSA. A combined encryption algorithm is proposed in this thesis. That is, the algorithm security is greatly improved. The combined encryption algorithm is completely validated, and its security is very high.

Steps of Algorithm for Key Generation:

1. Choose two distinct prime numbers P and Q.
2. Calculate N = P x Q. (n is used as mod for both the public and private keys).

3. Select the public key (i.e. encryption key) E such that it is not a factor of (P – 1) and (Q - 1).
4. Select the private key (i.e. the decryption key) Dsuch that the following equation is true (D x E) mod (P – 1) x (Q – 1) = 1.
5. For encryption, calculate the cipher text Cfrom the plain text PT as follows:

   CT = PTEmod N.
6. Then send CT as the cipher text to the receiver.
7. For decryption, calculate the plain text PT fromthe cipher text CT as follows:

   PT = CTD mod N.

1.3 Diffie-Hellman Algorithm

Whitfield Diffie and Martin Hellman discovered what is now known as the Diffie-Hellman (DH) algorithm in 1976. It is an amazing and ubiquitous algorithm found in many secure Connectivity protocols on the Internet. Diffie–Hellman establishes a shared secret key that can be used for secret communications by exchanging data over a public network. The purpose of the algorithm is to enable two users to securely exchange a key that can then be used for subsequent encryption of messages. The algorithm itself is limited to the exchange of secret values. This shared secret is important between two users who may not have ever communicated previously, so that they can encrypt their communications.

Steps of this Algorithm are as:

1. Taking two numbers “P” and “G” “P” is a largeprime number “G” is called the base.
2. Picks a secret number “A” as first secretnumber = A, then picks another secret number“B” as second secret number = B.
3. Computes first public number X = GA mod P,and public number = X. Then computes secondpublic number Y = GB mod P, and publicnumber = Y.
4. Exchange their public numbers.
5. First knows P, G, A, X, Y, Second knows P, G,B, X, Y.
6. Computes First session key as KA = YA mod P OR KA = (GB mod P) A mod P OR KA = (GB)A mod P OR KA = GBA mod P.
7. Computes second session key as KB = XB modP OR KB = (GA mod P) B mod P OR KB =(GA) B mod P OR KB = GAB mod P.

8. Fortunately for Both by the laws of algebra,First session key “KA” is the same as Secondsession key “KB”, or KA = KB = K.
9. Now, we have both the secret value as “K”.

2. Literature Survey

This section gives the detail of topic survey and review the work done by different authors in this field.

2.1 Overview

Yi Chen, Hong Chen, Hongqian, Chen, Xianchen Cheng [1] they first analyzed the characteristics of data and security problems in DIS network. For the real-time interactive data in DIS network, a stream cipher algorithm based on Logistic chaotic map (Logistic-EA) was presented. In this algorithm, the key stream was generated by Logistic chaotic map. The cipher text was gotten by executing XOR operation of plaintext and key stream. Logistic-EA has high security level and high encryption speed. For the non-real-time data, a hybrid encryption algorithm based on the chaos theory and AES (Chaos-AES) was presented. In this algorithm, the initial key and round key were generated by logistic chaotic map. Chaos-AES increased key space and implemented one-time pad. So that the cipher text encrypted by this algorithm is harder to break. The experiment results indicate that the algorithms above are effective in the DIS network.

Subhasis Mukherjee, MaynulHasan, Bilal Chowdhury, Morshed Chowdhury [2] the use of RFID (Radio Frequency Identification) technology can be employed for tracking and detecting each container, pallet, case, and product uniquely in the supply chain. It connects the supply chain stakeholders (i.e., suppliers, manufacturers, wholesalers/distributors, retailers and customers) and allows them to exchange data and product information. Despite these potential benefits, security issues are the key factor in the deployment. So they proposes a hybrid approach to secure RFID transmission in Supply Chain Management (SCM) systems using modified Wired Equivalent Encryption (WEP) and Rivest, Shamir and Adleman (RSA) cryptosystem.Their proposed system also addresses the common loop hole of WEP key algorithm and makes it more secure compare to the existing modified WEP key process

Kirtiraj B Hatele, Prof. AmitSinhal ,Prof. Mayank P Athak [3] They proposed hybrid security protocol architecture offeredhigh degree of security especially against square attacksand efficient in terms of time. The given plain text can be encrypted with the help of AES (Advance encryptionstandard) and the derived cipher text can be communicatedto the destination through any secured channel.Simultaneously the Hash value is calculated through MD5for the same plain text, which already has been convertedinto the cipher text by AES. This Hash value has beenencrypted with Dual RSA and the encrypted message ofthis Hash value also sent to destination.Now at the receiving end, hash value ofDecrypted plaintext is calculated with MD5 and then it iscompared with the hash value of original plaintext which iscalculated at the sending end for its integrity. By this it is able to know whether the original text being altered ornot during transmission in the communication medium. The intruders may try to hack the original information fromthe encrypted messages. Although intuder he may be able to trapboth the encrypted messages of plain text and the hashvalue but he will not be able to decrypt these messages toget original one. Hence the message can be communicatedto the destination in a highly secured manner.

Lili Yu, Weifeng Wang Zhijuan Wang [4] the combined encryption algorithm is successfullymade by using the initial encryption algorithm, Micro Genardencryption algorithm and the famous Base64 encryptionalgorithm. That is, in accordance with the order of the initialencryption algorithm, the improved Micro Genard encryptionalgorithm and the famous Base64 encryption algorithm, theuser’s information is gradually encrypted, and the algorithmsecurity is greatly enhanced. Besides, to video surveillancesoftware system for instance, which is widely used in the fieldof the traffic security management, the combined encryptionalgorithm is completely validated, and its security is very high.

Smita P. BansodVanita M. Mane Leena R. Ragha [5] this paper is based on hybrid cryptographic techniques based on DES and RSA algorithms to achieve data encryption and compression technique to store large amount of data. A combination of both provides superior security control. The suggested algorithm is modified BPCS (Bit Plane Complexity Segmentation) steganography technique that can replace all the “noise-like” regions in all the bit-planes of the cover image with secret data without deteriorating the image quality. According to the experiments, the messages can be successfully camouflaged in the cover image, and the stego images have satisfactory quality. Moreover, our scheme allows for a large capacity of embedded secret data and can be extracted from stego-image without the assistance of original image.

Adnan Abdul-Aziz Gutub, Farhan Abdul-Aziz Khan [6] proposes a hybrid crypto system that utilizes benefits of both symmetric key and public key cryptographic methods. Symmetric key algorithms (DES and AES) are used in the crypto system to perform data encryption. Public key algorithm (RSA) is used in the cryptosystem to provide key encryption before key exchange. Combining both the symmetric-key and public-key algorithms provides greater security and some unique features which are only possible in this hybrid system. The cryptosystem design is modelled using Verilog HDL. The implementation has various modules for DES, AES and RSA. The implementation also has a pseudorandom number generation unit for random generation of keys and a GCD computation unit for RSA. All the hardware modules are designed by Register Transfer Level (RTL) modelling of Verilog HDL using ModelSimSE 5.7e.

3. HYBRID ENCRYPTION

3.1 Limitations of RSA

- If any one of p, q, e, d is known, then the other values can be calculated. So secrecy is important.
- It is important to make sure that message lengthShould be less then bit length otherwise the algorithm will fail.
- Due to the usage of public key RSA is much slower than any other symmetric cryptosystems.
- The length of plain text that can be encrypted islimited to the size of n=p*q.
- Each time RSA initialization process requires the random selection of two very large prime numbers (p and q).

3.2 Limitations of Diffie Hellmen

- It is easily susceptible to man-in-the-middle attacks.
- The algorithm cannot be used to encrypt messages.
- There is also a lack of authentication.
- The computational nature of the algorithm couldbe used in a denial-of-service attack very easily.

3.3 Hybrid Encryption Algorithm on RSA and Diffie-Hellmen

Steps of this algorithm are as:-

1. Choose two large prime numbers P and Q.

   a. Calculate N = P x Q.

b. Select public key (i.e encryption key) E such that it is not a factor of (P – 1) and (Q -1).

c. Select the private key (i.e. the decryption key) D such that the following equation is true (D x E) mod (P – 1) x (Q – 1) = 1

d. Suppose R, S and G is automatic generated prime constants.

e. And put the value of E and D from above as secretnumber such that A=E and B=D.

2. Now calculate following as public number

X= GA mod R

Y= GB mod R

3. Calculate session key with formula

KA = YA mod R or KA = (GB mod R)A mod R or KA = (GB) A mod R or KA = GBA mod P.

KB = XB mod R or KB = (GA mod R)B mod R or KB =(GA) B mod R or KB = GAB mod R.

Such that KA = KB = K.

3. For Encryption we use session key K with Plain text PT that will generate a new Cipher text CT Then send CT as the cipher text to the receiver and for decryption, calculate the plain text PT from the cipher text CT.

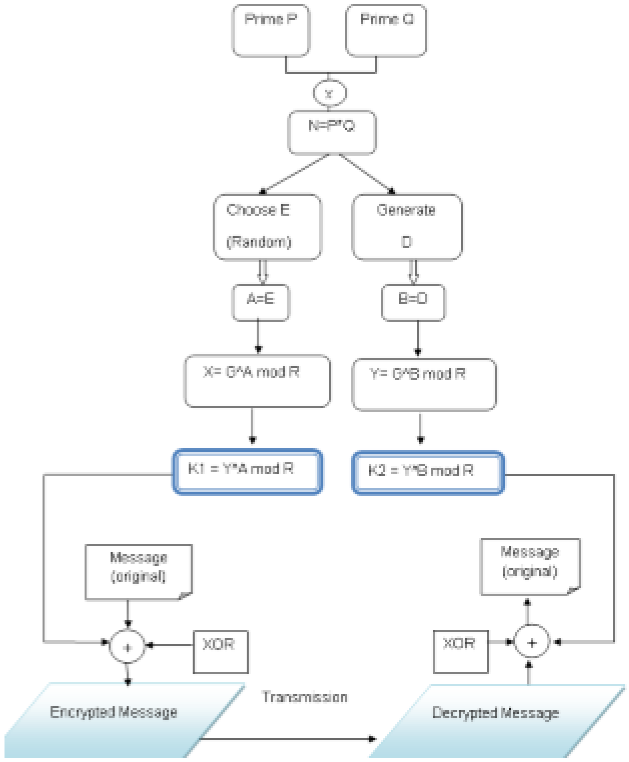

Figure 2: A Hybrid RSA &Diffie-Hellman [7]

4. Proposed Work

The security of the RSA cryptosystem is based on two mathematical problems: the problem of factoring large numbers know mathematical attack and the problem of trying all possible private keys know brute force attack. So to improve the security, this scheme presents a new cryptography called Improved RSA (IRSA). IRSA is secure as compared to RSA as it is based on the factoring problem as well as decisional composite residuosity assumptions which is the intractability hypothesis. The scheme is an additive homomorphic cryptosystem; this means that, given only the public-key and the encryption of m1 and m2, one can compute the encryption of m1 + m2.

4.1 Improved RSA

IRSA4 is an asymmetric-key cryptosystem, meaning that for communication, two keys are required: a public key and a private key. Furthermore, unlike RSA, it is one way, the public key is used only for encryption, and the private key is used only for decryption. Thus it is unusable for authentication by cryptographic signing. Here '4' indicates that this RSA uses four prime numbers to increased mathematical complexity for the attackers.

Following is a key generation algorithm for IRSA cryptosystem.

A. Key Generation Algorithm:

1. Choose four large prime numbers p, q, r and s randomly and independently of each other. All primes should be of equivalent length.
2. Compute $n = p * q$, $m= r * s$, $\varphi= (p-1) * (q-1)$ and $\lambda =(r-1) * (s-1)$.
3. Choose an integer e, $1 < e < \varphi$, such that $\gcd (e, \varphi) = 1$.
4. Compute the secret exponent d, $1 < d < \varphi$, such that $e * d \bmod \varphi =1$.
5. Select an integer $g=m+1$.
6. Compute the modular multiplicative inverse: $\mu = \lambda^{-1} \bmod m$.
7. The public (encryption) key is (n, m, g, e).
8. The private (decryption) key is (d, λ, μ).

B. Encryption:

1. Let m be a message to be encrypted where 0<mesg< n.

2. Select random r where $r < m$.

3. Compute ciphertext as: $c=g^{mesg\text{^}e \bmod n} * r^m \bmod m^2$.

C. Decryption

1. Compute message: $m = (((c^{\lambda} \bmod m^2 – 1)/ m) * \mu \bmod m)^d \bmod n$

4.2 Example of Improved RSA

1. Choose four large prime numbers p, q, r and s randomly and independently of each other. All primes should be of equivalent length. p=3, q=5, r=7, s=2

2. Compute $n = p \times q=15$, $m= r \times s=14$, $\varphi= (p-1) \times (q-1)=8$ and $\lambda=(r- 1) \times (s-1)=6$.

3. Choose an integer e, $1 < e < \varphi$ such that $\gcd (e, \varphi) =1$ e=7

4. Compute the secret exponent d, $1 < d < \varphi$, such that $e \times d \bmod \varphi =1$.
   d=7

5. Select an integer g=m+1. g=15

6. Compute the modular multiplicative inverse: $\mu=\lambda$ -1 mod m.μ=5

The public (encryption) key is (n, m, g, e) (15, 14, 15, 7)

The private (decryption) key is (d, λ ,μ) (7, 6, 5)

Encryption:

Plaintext s=5

Select random number r, where r < m.

r=13

Compute cipher text as: $c=g^{s\wedge emodn} * r^{m} \bmod m^{2}$.

$c=15\wedge 78125 \times 3937376385699289 \bmod 14^{2}$

Now here onwards large calculations

Decryption:

Compute original message:

$m = (((c^{\lambda} \bmod m^{2} - 1)/ m) * \mu \bmod m)^{d} \bmod$

4.3 Proposed Algorithm

Moreover, Internet and Network applications have seen a tremendous growth in the last decade. As a result incidents of cyber attacks and compromised security are increasing. This requires more focus on strengthening and securing our communication. One way to achieve this is cryptography. Although a lot of work has been done in this area but this problem still has scope of improvement. In this paper we have focused on asymmetric cryptography and proposed a novel method by combining the IRSA4 and Diffie-Hellman in order to achieve more security called as Improved RSA with Diffie-Hellman using 4 prime numbers IRDH4.

Steps of this algorithm are as:

1. Choose four large prime numbers p, q, r and s randomly and independently of each other. All primes should be of equivalent length.

Compute $N = P * Q$, $M= R * S$, $\varphi= (P-1) * (Q-1)$ and $\lambda =(R-1) * (S-1)$.

Choose an integer e, $1 < e < \varphi$, such that $\gcd (e, \varphi) = 1$.

Compute the secret exponent d, $1 < d < \varphi$, such that $e * d \bmod \varphi =1$.

Select an integer $G=M+1$.

Compute the modular multiplicative inverse: $\mu = \lambda^{-1} \bmod m$.

And put the value of e and d from above as secret number such that A=e and B=d.

2. Now calculate following as public number

$X=G^{A} \bmod R$

$Y= G^{B} \bmod R$

3. Calculate session key with formula

KA = Y^A mod R or KA = $(G^B$ mod $R)^A$ mod R or KA = $(G^B)^B$ mod R or KA = G^{BA} mod P.

KB = X^B mod R or KB = $(G^A$ mod $R)^B$ mod R or KB = $(G^A)^B$ mod R or KB = G^{AB} mod R.

Such that KA = KB = K.

4. For Encryption we use session key K with Plain text PT that will generate a new Cipher text CT Then send CT as the cipher text to the receiver and for decryption, calculate the plain text PT from the cipher text CT.

Firstly to use Improved RSA each user must (privately) choose fourlarge random numbers P,Q,R and S to create his ownencryption and decryption keys. These numbers must belarge so that it is not computationally feasible for anyone tofactor N = P*Q,M=R*S**.** Next step is to generate E andD. After this we put E and D as inputs A and B to Diffie-Hellman and compute XA and XB , through which wegenerate session key KA and KB such that KA = KB = K.Then we XOR our input Plain text with the session key (K)for Encryption or to produce Cipher text and forDecryption again XOR Cipher text with session key (K) toproduce original Plain text.

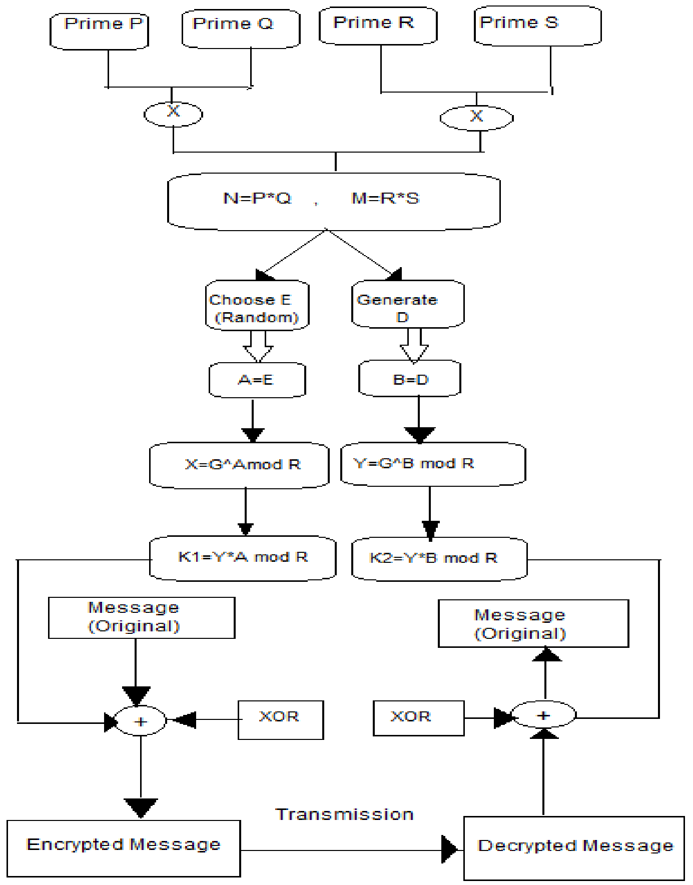

Figure 3: A Hybrid Improved RSA &Diffie-Hellman

5. Comparative Study

The Improved RSA cryptosystem is based on additive homomorphic properties and RSA cryptosystem, additive homomorphic scheme required four prime numbers, itwill be more difficult and take long time to factor dualmodulus, so one have to factor the dual modulus into its four primes to break the IRSA algorithm .If RSAwhich is based on single modulus, is broken in time x an dadditive homomorphic based on dual modulus, is brokenin time y then the time required to break IRSA algorithmis x*y. So the security of IRSA algorithm is increased ascompare to RSA algorithm and it shows that the IRSA algorithm is more secure for ***Mathematical attacks***. As in IRSA double decryption is performed and unlikeRSA that is not only based on private key but also basedon the subset sum problem so one can't break Improved RSA only guessing the private key only. So it shows that Improved RSA algorithm is more secure as compare to RSA for ***Brute force attack.***

6. Future Work

The proposed approach will be of great use for the securecommunication. It will be easy for user to send and receivemessages and files which are the most confidential to them. Presently, the usability of proposed Algorithm is given with veryfew concept and ideas which in future can be expand. Theefficiency in terms of time complexity can be revised forbetter working of algorithm. The key size for encryptionand decryption purpose can be reduces further. Currently the Algorithm is used for encryption and decryptionpurpose only. Further it can be used for digital signature generation.

7. Conclusion

Data confidentiality and security have become the prime aspects in today's world of fast communication. Internet has played a vital role in bringing the world closer but at the same time has posed many challenges from data security and integrity point of view. After research across all the available material and techniques it was found that there is still lot work to be done in order to ensure data integrity. Keeping this in mind in this paper it has been tried to combine two of the best security algorithm RSA and Diffie-Hellman. Further we proposed a novel method, to strengthen the security aspect, by comparing both these algorithms and providing with the best of these two algorithms. It mainly concentrates on asymmetric cryptography by combining the IRSA and Diffie-Hellman in order to achieve more security called as Improved RSA with Diffie-Hellman using 4 prime numbers IRDH4. Moreover, still this area is continuous evolving and needs more work to be done on continuous basis.

8. References

[1] Yi Chen, Hong Chen, Hongqian, Chen, Xianchen Cheng-"Research on Data Encryption Techniques for Distributed Interactive Simulation Network", International Conference on Computer Application and System Modeling, IEEE 2010.

[2] Subhasis Mukherjee1, MaynulHasan, Bilal Chowdhury, Morshed Chowdhury-" Security of RFID Systems - A Hybrid Approach", 12th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, IEEE 2011.

[3] Kirtiraj B Hatele, Prof. Amit Sinhal, Prof. Mayank P Athak-"A Novel Approach to the Design of a New Hybrid Security Protocol Architecture", International Conference on

Advanced Communication Control and Computing Technologies (ICACCCT), IEEE 2012.

[4] Lili Yu, Weifeng Wang, Zhijuan Wang-“The Application of Hybrid Encryption Algorithm in Software Security”, Fourth International Conference on Computational Intelligence and Communication Networks, IEEE 2012.

[5] Smita P. BansodVanita M. Mane Leena R. Ragha-“ Modified BPCS steganography using Hybrid Cryptography for Improving Data embedding Capacity”, International Conference on Communication, Information & Computing Technology (ICCICT), Oct. 19-20, Mumbai, India, IEEE 2011.

[6] Adnan Abdul-Aziz Gutub, Farhan Abdul-Aziz Khan-“Hybrid Crypto HardwareUtilizing Symmetric-Key & Public-Key Cryptosystems**”,** International Conference on Advanced Computer Science Applications and Technologies,
IEEE 2012.

[7] Shilpi Gupta , Jaya Sharma-“A Hybrid Encryption Algorithm based on RSA and Diffie-Hellman”, International Conference on Computational Intelligence and Computing Research, IEEE 2012.

[8] William Stallings, Cryptography and Network Security Principles and Practice, fifth Edition, Pearson publication.

[9] Vishal Garg, Rishu, Improved and Diffie Hellman Algorithm for Network Security Enhancement, Int.J. Computer Technology &Applications, Vol 3 (4), 1327-1331.

[10] Ravi Shankar Dhakar, Amit Kumar Gupta-“ Modified RSA Encryption Algorithm”, 2012 Second International Conference on Advanced Computing & Communication Technologies,IEEE 2012