Security Issues in Networks and its Solution at Architecture Level

Anudeep Randhawa
M.Tech Student
Depatment of Computer Science
RIEIT, Punjab(INDIA)

Heena Gulati
Assistant Professor
Depatment of Computer Science
RIEIT, Punjab (INDIA)

Harish Kundra
HOD(CSE&IT)
Department of Computer Sc. & IT
RIEIT, Punjab (INDIA)

ABSTRACT

Network infrastructure involves a variety of geographically distributed data sources, computational resources, storage systems, and databases and works as a unified integrated resource. Due to this security problems become an urgent and complex undertaking for the network applications. 512 bit RSA in today environment has become vulnerable to attacks and is considered no more secure. In order to secure data or information over a network we need to study different possible security issues in networks and to study how security issues affect the network performance. We will be investigating various solutions to these security issues and purpose an architectural based algorithm for providing security. We hereby will present an algorithm based on random alphanumeric string concatenation with addition to using *n* prime numbers. The idea behind this new technique is to provide maximum security for data by applying random alphanumeric string concatenation instead of ordinary integers over the network. Using combination of two different keys mechanism we will encrypt the plaintext twice. This will help to secure the data even if one succeeds to have an access to others private key Also we used *n* prime number which is not easily breakable and are difficult to decompose. This technique provides more efficiency, security and reliability over the networks.

Keywords

N prime numbers, encryption, random alphanumeric string concatenation, decryption

1. INTRODUCTION

In a network, there are number of entities that have to be authenticated such as users, resources and services. Authorization and access control are of vital importance in all networks. Network security's ultimate goal is to make a its infrastructure seamless and protect it against both known and unknown security attacks. According to this, we need a comprehensive analysis of existing network security issues and available countermeasures. Kernel level sandboxing techniques are very secure and can potentially answer all security concerns, but this solution can also result in extreme complexity. In network, where the computational, storage and resources are inherently heterogeneous, dynamic and multi-organizational in nature, the issue of managing security of both resources and users are most challenging.

In our proposed technique we used concept of using two different key in combination for encryption as well as decryption along with random alphanumeric string concatenation. It will also handle [1] *n* prime numbers combination of which provides high security.

2. BACKGROUND

Any system's security goal is to provide easy access to legitimate users and to prevent users who don't have the proper privileges from accessing resources and information. This section presents the traditional security threats that play an important role in defining security for network and the associated technologies.

2.1 User Threats

When user fundamental security mechanism like authentication or authorization are not carried out properly, there is a chance that different user threats will generate, hackers being the most common.

2.2 Mediator threats

During communication between user and service or resource provider there may be a mediator threat. So mediator threat consists of those threats originating from insecure service level communication.

2.3 Service Provider Attack

The service provider takes the job submitted by user, process them and send back the result to user with quality-of-service. So service threats are those kinds of threats that composed of malicious input to get malicious goal like malicious code/malware.

3. NEED OF SECURITY

Security becomes urgent need over the network firstly because if data is encrypted then the device that uses it doesn't need to be secure. This means that storage or transportation of it doesn't need to be securing which saves you money on extra protection software. Secondly, having the data encrypted it takes away the pain and worry that is associated with data breaches and the protection of intellectual property. It keeps data from snoopers without compromising systems or storage devices.

4. BASIC SECURITY REQUIREMENTS IN A NETWORK

With the use of internet is increasing in our day to day life for the daily works like sending e-mails the security of the data over the network is also required thus the data that is to be transmitted should be secure and inaccessible to the other user's of the network who are unauthorized for the access of that data. Various encryption and decryption methods are used to transfer data over the network. Encryption is done in fields basically related to military purposes, bank transactions and government officials such as to protect data and save the information from unauthorized access. The methods used for encryption are: Symmetric key encryption (private key encryption), Combination of both public and private key is asymmetric key encryption. In asymmetric encryption there are two keys: a private key and a public key.[2] The private key is kept by the receiver and the public key is announced to the public.

4.1 Information security

Secure communication issues include those security concerns that arise during communication between two entities: such as resources and users in a network, including Confidentiality, authentication and integrity. Confidentiality is mostly associated with encryption and provides information secrecy. Integrity offers protection from unauthorized modification of data. Authentication is the verification procedure of the identification of an entity in a system. [3]In a network, there are number of entities that have to be authenticated such as user, resources and services. Information security issues exist in all fields of computing and communications; researchers have studied them for quite some time.

4.2 Authentication

Network security requirements should contain authentication mechanisms at the entry point of the network system. Authentication deals with verification of the identity of an entity with in a network. An entity may be a resource provider, a user or service provider.

3.3 Authorization

After authentication, [4] the second most fundamental challenge to security in a network is authorization. Once the identity of a user can be established, it then becomes necessary to determine the permission of that user to use a particular resource.

4.4 Single sign-on

A single computation may require access to many resources and many times, but requiring a user to re-authenticate on each occasion is impractical and generally unacceptable. Single sign-on and delegation capabilities by creating a proxy (consisting of a new certificate and a new private key) so that user should be able to authenticate once and assign to the computation the right to operate on his/her behalf , typically for specified period and the time duration after which others should no longer accept the proxy.

4.5 Secure Communication

Security communication provides the ability for two or more entities to conduct a conversation on integrity, confidentiality and non-repudiation data communication.

5. LITERATURE REVIEW

Rivest, Adi Shamir and Leonard Adleman are the developer of the RSA, who first proposed this algorithm 1977[5][6]. This is an algorithm for cryptography that is based on the difficulty of factoring large integers. The prime factors must be kept secret. [7]Anyone can use the public key to encrypt a message but this message can only be decrypted using the private key which is held only on the receiver side for whom message is intended. If the public key is large enough, only someone with knowledge of the prime factors can feasibly decode the message. Attacks can be launched by encrypting likely plaintexts under the public key and test if they are equal to the cipher text.

Traditional RSA involves a public key and a private key. [8] The public key is known to everyone and is used for encrypting messages while decryption is done using the private key. The keys for the RSA algorithm are generated the following way:

RSA algorithm

1. Generate two large random primes p and q, $n = pq$
2. Compute $n = pq$ and (phi) $\varphi = (p-1)(q-1)$.
3. Choose an integer e, $1 < e < phi$, such that $gcd(e, phi) = 1$.
4. Compute the secret exponent d, $1 < d < phi$, such that $ed \equiv 1\ (mod\ phi)$.
5. The public key is (n, e) and the private $key\ (d, p, q)$. Keep all the values d, p, q and phi secret.
6. Convert the message m into integer such that $1 < m < n$
7. Encrypt m using $c = m^{e}\ mod\ n$ to obtain cipher text
8. Decrypt m using $c^{d}\ mod\ n$ to obtain original message.

- n is known as the modulus.
- e is known as the public key component.
- d is known as the secret key component.

A working example

- Select prime numbers p=11, q=3.
- $n = pq$ = 11.3 = 33
  $phi = (p-1)(q-1)$ = 10.2 = 20
- Choose e=3
  Check $gcd(e, p-1)$ = gcd(3, 10) = 1 (i.e. 3 and 10 have no common factors except 1), and check $gcd(e, q-1)$ = gcd(3, 2) = 1 therefore gcd(e, phi) = $gcd(e, (p-1)(q-1))$ = gcd(3, 20) = 1
- Compute d such that $ed = 1\ (mod\ phi)$ i.e. find a value for d such that phi divides (ed)-1 i.e. find d such that 20 divides $3d - 1$. Simple testing (d = 1, 2, ...) gives d = 7 Check: ed-1 = 3.7 - 1 = 20, which is divisible by phi.
- Public key = (n, e) = (33, 3) and Private key = (n, d) = (33, 7).
- Now say we want to encrypt the message m = 7, $c = m^{e}\ mod\ n$ = 7^{3} mod 33 = 343 mod 33 = 13. Hence the ciphertext c = 13.
- To check decryption we compute $m' = c^{d}\ mod\ n$ = 13^{7} mod 33 = 7.

6. PROBLEM DEFINITION

As the users are from number of different organizations, each organization may have different access policies and security mechanisms. Maintaining security in such an environment is a real challenge and most difficult part is security management of large high speed networks. In networks, data may be vulnerable to attacks and threats hence this can be minimized or removed using security prospective. Thereafter, a new modified version of RSA was proposed in which the cipher text obtained with the help of public key was appended with an ordinary integer i.e. a number. And accordingly plain text was obtained using the private key after removing that ordinary integer. It was somewhat secure as compared to that of Traditional RSA.

Modified RSA

The classical RSA algorithm has been modified. It was proposed that this modification is reliable and more secure than the classical RSA. But the usage of ordinary number may still cause security problems The [9] modified version of the traditional RSA is as follows:

1. Generate two large random primes p and q, $n = pq$
2. Compute $n = pq$ and (phi) $\varphi = (p-1)(q-1)$.
3. Choose an integer e, $1 < e < phi$, such that $gcd(e, phi) = 1$.
4. Compute the secret exponent d, $1 < d < phi$, such that $ed \equiv 1\ (mod\, phi)$.
5. The public key is (n, e) and the private $key\ (d, p, q)$. Keep all the values d, p, q and phi secret.
6. Convert the message m into integer such that $1 < m < n$
7. Encrypt m using $c = m^{e}\, mod\, n$ to obtain cipher text
8. Append with the ordinary integer say I into c using $c' = c + I$
9. Now remove this ordinary integer i.e. I at receiver side as $c = c' - I$
10. Decrypt m using $c^{d}\, mod\, n$ to obtain original message.

A working example

- Select prime numbers p=11, q=3.
- $n = pq$ = 11.3 = 33
  $phi = (p-1)(q-1)$ = 10.2 = 20
- Choose e=3
  Check $gcd(e, p-1) = gcd(3, 10) = 1$ (i.e. 3 and 10 have no common factors except 1), and check $gcd(e, q-1) = gcd(3, 2) = 1$ therefore gcd(e, phi) = $gcd(e, (p-1)(q-1)) = gcd(3, 20) = 1$
- Compute d such that $ed = 1\ (mod\, phi)$ i.e. find a value for d such that phi divides (ed)-1 i.e. find d such that 20 divides $3d - 1$. Simple testing (d = 1, 2, ...) gives d = 7 Check: ed-1 = 3.7 - 1 = 20, which is divisible by phi.
- Public key = (n, e) = (33, 3) and Private key= (n, d) = (33, 7).
- Now say we want to encrypt the message m = 7, $c = m^{e}\, mod\, n = 7^{3}\, mod\ 33 = 343\, mod\ 33 = 13$. Hence the ciphertext c = 13.
- Append c with a ordinary integer say 1
  c'= 13+1=131
- Remove the ordinary integer appended to c'
  c=131-1 =13
- To check decryption we compute $m' = c^{d}\, mod\, n = 13^{7}\, mod\ 33 = 7$.

7. PROPOSED WORK

Network security is one of the most crucial and difficult research topics. It is ultimate goal is to make the network infrastructure seamless and protect it against both known and unknown security attacks. Networks weather distributed or grid helps us overcome [3] heterogeneity in terms of computing elements, operating systems, policy decisions and environment. However, security issues always occur. We proposed to device a model using c# under architectural level categorization to be widely adopted in order to serve as a foundation for further defining access control requirements, analysis of security issues and their solutions in a network. We need a comprehensive analysis of existing network security and available countermeasures. Our work on architectural level based upon various security issues and their solution. These mainly contain information security. Here we use combination of two keys for encryption. Key used in a combination are much more safer than that of when key are used individually. Because it becomes a cumbersome task for the hacker to guess when key are used in combination providing data much more security.

7.1 SOLUTION METHODOLOGY

In our technique we used concept of encrypting data twice along with random alphanumeric string stuffing and usage of n prime number which is not easily breakable as these cannot easily decompose. This provides more efficiency, security and reliability over the networks. Here we are used architectural based algorithm to bring about ciphertext concatenation with a random string and to handle n prime numbers (non-repeatable) which provides high security. This take place in two steps: encryption and decryption. Encryption which is used to convert original (plain text) data to cipher text concatenated with a random string. The plain text is said to be clear text and is easily read by anyone. Second in decryption, which is used to convert cipher text to deconcatenated cipher text and then decrypt to plaintext (readable format).We implemented positive justification or stuffing in our data transmission. Random string stuffing is the non-information string inserted into data for security purposes. The location of the stuffing this random string is communicated to the receiving end of the data, where these extra bits are removed to return the original string. We will use it as the string which are not important for messaging but will be useful for security. This extra random string will confuse the attacker and he will not be able to determine it.

Fig 1 represents the proposed flowchart diagram for our proposed algorithm. From the below diagram, it is very clear that secure communication which will occur between receiver and sender because of random string S stuffing in the ciphertext. We are using two key combination comprising K1 and K2. Public and private key will be used to encrypt twice the plaintext into ciphertext while reverse would be used to decrypt the ciphertext back into plain text.

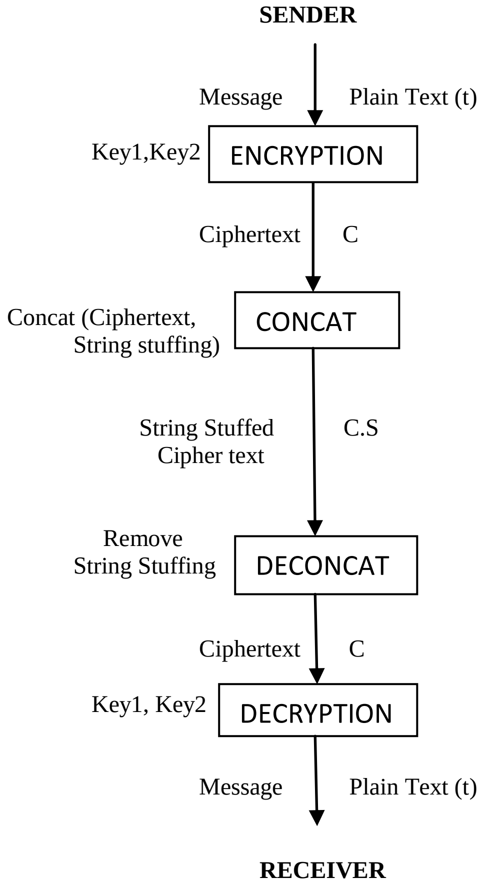


Figure 1. Working of the algorithm

Proposed Algorithm

1. Random prime numbers, $w\,x\,y\,v$ are generated, usually having equal size such that their product $n = wxyv$
2. Now we will compute (phi) $\varphi = (w-1)(x-1)\,(y-1)(v-1)$.
3. Choose an integer i, $1 < i < phi$, such that $f(i, phi) = 1$.
4. Now to compute the secret component z, $1 < z < phi$, where $iz \equiv 1\ (mod\ phi)$.
5. Now (n, i) is the public key and the private key is (z, w, x, y, v). Values z, x, y and phi are kept secret.
6. First convert message M into an integer say 't', such that $0 < t < n$ with the help of padding scheme
7. Then he will compute the ciphertext 'C' using both the keys i and z corresponding to $C = E_i(D_z(E_i(t)))$ where E is encrypting and D is used for decryption. Now the encrypted ciphertext comes out to be

   $E_i(t) = t^i\ (mod\ n)$

   $D_z(E_i(t)) = E_i(t)^z(\ mod\ n)$

   $C = E_i(D_z(E_i(t))) = D_z(E_i(t))^i(mod\ n)$
8. Add the random string S into C using

   $C` = Concat(C,S)$
9. Now remove random string S at receiver side as

   $C = C` - S$
10. Reverse comes the process of decryption. With the help of private key component 'z' can recover 't' from 'C', computing $t = D_z(E_i(D_z(c)))$ by using both keys i and z where E is for encryption and D is for decryption

    $D_z(C) = c^z(mod\ n)$

    $E_i(D_z(C))) = D_z(C)^i(mod\ n)$

    $t = D_z(E_i(D_z(C))) = E_i(D_z(C)))^z(mod\ n)$

- S is a alphanumeric random string.

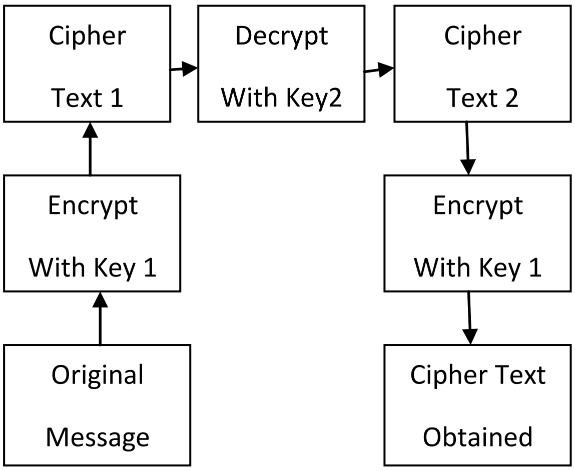


Figure 2. Encryption Process

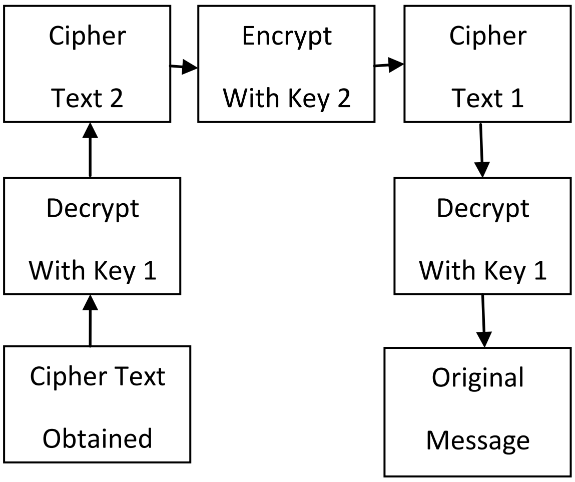


Figure 3. Decryption Process

Case Study

- Select four prime numbers. Calculate $n = w * x * y * v$
  w=2, x=3, y=5, v=17. n=2*3*5*17=510

- Calculate $f(n) = (w-1)(x-1)(y-1)(v-1)$
  f(510) = (2-1) (3-1) (5-1)(17-1) =128
  f (n)=128

- Select any number i, 1<i<128

- F (n) must not be divisible by i, Let i=3
- Calculate z, such that 128 divides 3z-1.
  Simple testing (z = 1, 2,) gives z= 43. Now check iz-1 = 3*43 - 1 = 128, which is divisible by phi.
  z= 43

- the public key is(n = 510, i = 3)
- private key is (n = 510,z = 43)

- Given message t= 11.

- Encryption: $E_{\mathrm{i}}(D_{\mathrm{z}}(E_{\mathrm{i}}(t)))$

- Now Key1=i=3 and Key2=z=43

- Encrypt using i where i=3
  $E_{\mathrm{i}}(t)$ =11^3 mod 510
  $E_{\mathrm{i}}(t)$ = 1331 mod 510 = 311
  $E_{\mathrm{i}}(t)$ = 311

- Now decrypt using z where z=43
  $D_{\mathrm{z}}(E_{\mathrm{i}}(t))$=$311^{43}$ mod 510 = 11
  $D_{\mathrm{z}}(E_{\mathrm{i}}(t))$=11

- Again Encrypt using i where i=3
  $E_{\mathrm{i}}(D_{\mathrm{z}}(E_{\mathrm{i}}(t)))$=$11^3$ mod 510
  $E_{\mathrm{i}}(D_{\mathrm{z}}(E_{\mathrm{i}}(t)))$ =1331 mod 510 = 311

- Finally $C = E_{\mathrm{i}}(D_{\mathrm{z}}(E_{\mathrm{i}}(t)))$ = 311

- Now the generated random alphanumeric string S is let's saying 1a2+b#7. **Concatenate** it in the C' on particular defined position as follows:
  $$C` = Concat(C, S)$$
  $C`$=3111a2+b#7

- To decrypt the cipher text, firstly we have to remove the S from $C`$ as
  $$C = C` - S$$
  C=3111a2+b#7-S
  C=311

- Decryption: $D_{\mathrm{z}}(E_{\mathrm{i}}(D_{\mathrm{z}}(C)))$

- Now Reverse operation goes as: Key1=z=43 and Key2=i=3

- Decrypting using z where z=43
  $D_{\mathrm{z}}(C)$= 311^{43} mod 510 = 11

- Now encryptin using i=3
  $E_{\mathrm{i}}(D_{\mathrm{z}}(C))$= 11^3 mod 510
  $E_{\mathrm{i}}(D_{\mathrm{z}}(C))$= 1331 mod 510 = 311

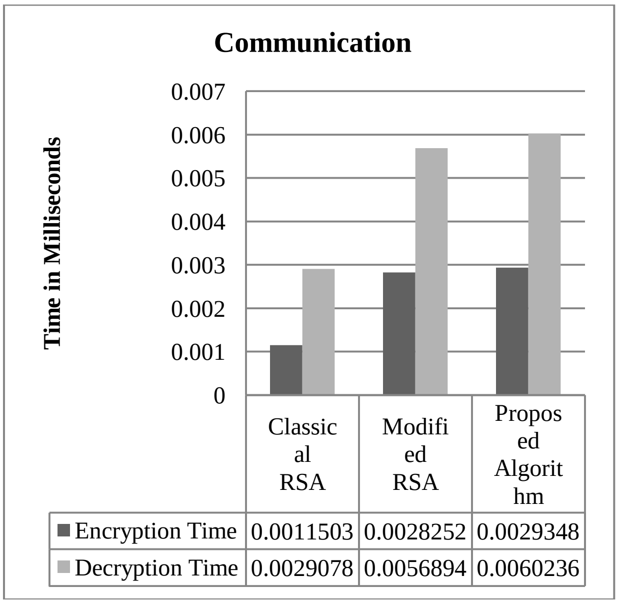
- Again decrypting using z where z=43
  $D_{\mathrm{z}}(E_{\mathrm{i}}(D_{\mathrm{z}}(C)))$= 311^{43} mod 510 = 11

- Finally $t = D_{\mathrm{z}}(E_{\mathrm{i}}(D_{\mathrm{z}}(C)))$=11 which was the original message

We also used n prime numbers which is provided the security over the networks.

8. COMPARATIVE STUDY OF ABOVE MENTIONED ALGORITHMS

Here in this section, we evaluate the run time of the classical, modified RSA and proposed algorithm by showing the run time results through a server client communication. In the said figure, we take a conversation message through a network communication. In the Figure 4 given below, server sends a message to client through a network.



	Classical RSA	Modified RSA	Proposed Algorithm
■ Encryption Time	0.0011503	0.0028252	0.0029348
■ Decryption Time	0.0029078	0.0056894	0.0060236

Figure 4. Comparison of Encryption and Decryption time taken by the above discussed algorithms during message passing over a network in milliseconds.

Thus here we observe that in the process of communication between Server and Client that:

- The time taken by Classical RSA to encrypt message "Hello Client, Welcome to our network" is 0.0027693 milliseconds. While for that of decryption of the same takes 0.0049078 milliseconds.

- The time taken by Modified RSA to encrypt message "Hello Client, Welcome to our network" is 0.0028252 milliseconds. While for that of decryption of the same takes 0.0056894 milliseconds.

- The time taken by Proposed Algorithm to encrypt message “Hello Client, Welcome to our network” is 0.0029348 milliseconds. While for that of decryption of the same takes 0.0060236 milliseconds.

Table1: Comparative Study of Proposed Algorithm

Sr No.	**Traditional RSA**	**Modified RSA**	**Proposed Algorithm**
1.	Uses two prime numbers	Uses two prime numbers	Uses n prime numbers
2.	Less Time for execution	More executing time than traditional RSA	More execution time
3.	Suited for multi user environment	Suited for multi user environment	Suited for multi user environment
4.	Less secure	secure to some limit	Most secure
5.	Less complexity	Less complexity	Little bit complex

9. CONCLUSION

In this paper we have proposed the combination of two different keys used in the process of encryption along with random string concatenation and n prime numbers in combination which has provided the security over the networks. Addition to that we used non-repeatable prime numbers for even more secure communication. These play a vital role to secure data. **Data protection:** Plain text message would be converted to cipher text and simultaneously string stuffed to give plain data a extra protection cover. **Confidentiality:** This model not will guarantee the confidentiality of information and keep sensitive data secure. **Authorization:** Encrypted password can only be read by a system or user who has the key to decrypt the data means the system or user is authorized to read the data. **Authentication:** Only those user are allowed the access of system who will identify themselves with username and protected password. **Threat from Hackers:** Encrypting password and encrypted cum string stuffed messages will keep all but the most dedicated hackers away from intercepting and reading secret data.

10. ACKNOWLEDGMENTS

My thanks to my teachers, who have contributed towards development of the research paper. Also I would like to pay my regard to my sister and parents for their contribution

11. REFRENCES

[1] B.Persis Urbana Ivy, Purshotam Mandiwa and Mukesh Kumar, 2012 A modified RSA cryptosystem based on ‘n’ prime numbers.

[2] Soram Ranbir Singh, Khomdram Memeta Chanu,Elliptic Curve Public-Key Cryptosystem Over Z(i), International Journal of Computer Science & Engineering Technology (IJCSET)

[3] Chakrabarti, Damodaran,A. and Sengupta,S.2008 Grid Computing Security: A Taxonomy. IEEE Computer Society Jan.-Feb. 2008, PP44-51.

[4] Nirbhay Ahlawat, Sangram Bana and Chetan Sharma, 2012 A Difference Disclosure Method for DDoS Attack in Grid Computing.

[5] Wikipedia. RSA online :http://en.wikipedia.org/wiki/RSA

[6] Dr Clifford Cocks CB". Bristol University. Retrieved 2011-08-14.

[7] Rivest, R.; A. Shamir; L. Adleman (1978). "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems". Communications of the ACM 21 (2): 120–126.

[8] K. Sathish Kumar, R. Sukumar, S. Kharthikeyan Efficient Authentication Protocols for Mobile Hand-held Devices with Minimum Power Consumption IOSR Journal of Computer Engineering (IOSR-JCE) Volume 9, Issue 2 (Jan. - Feb. 2013), PP 41-45

[9] Parshotam, Rupinder Cheema and Aayush Gulati “Improving the Secure Socket Layer by Modifying the RSA Algorithm” International Journal of Computer Science, Engineering and Applications (IJCSEA) Vol.2, June 2012