



Amalgamation of Cryptographic Techniques for Secured Data Transmission

Meghana V¹, Aishwarya B¹, Shobha M.S²

B.E. Student, Department of ISE, NHCE, Bangalore, Karnataka, India¹

Senior Assistant Professor, Department of ISE, NHCE, Bangalore, Karnataka, India²

ABSTRACT: Data security plays a vital role in the Internet which is a public-interacted system. The amount of information exchanged over the internet is completely not safe. Protecting the information transmitted over the network is a difficult task and the data security issues become increasingly important. There are symmetric key encryption techniques which use only one key for both encryption and decryption of the data. They are simple in design but can be easily cracked using brute force attacks. The entire security of such a cipher could be compromised if the attacker any how gets access to the keys. On the other hand, there are asymmetric key based algorithms which use a pair of keys, one for encryption, and the other for decryption, whose security is higher as compared to the symmetric ones but lack in time efficiency. It is also difficult to manage such a huge base of key-pairs efficiently and safely. This paper mainly focuses on the implementation of a system capable of encryption and decryption of data using a hybrid model based on the amalgamation of symmetric encryption techniques such as AES and asymmetric techniques such as RSA. This new hybrid cryptographic algorithm has been designed for better security with integrity without compromising on the speed and efficiency.

KEYWORDS: Symmetric encryption, asymmetric encryption, hybrid encryption

I. INTRODUCTION

Cryptography plays a vital role in data security. It has become more critical to our day to day life since most of the data transactions take place electronically via email, ATM, cellular phones etc. One of the most significant communication means being emails, Since all the business and financial transactions takes place through the same it is important to enable high security without compromising efficiency.

Currently emails have been using PGP, AES, RSA, blowfish, triple DES, twofish algorithms for encryption. In this paper, we use the combination of AES and RSA algorithm with a layer of authentication provided by digital signature. The entire working of the system enables faster encryption of huge data without having exposed to attacks and overcoming drawbacks of both the algorithms mutually to provide a strong and efficient data security scheme for emails.

II. RELATED WORKS

In [2] authors have discussed about cryptography, where they encode data before sending it and decode it on receiving, for this purpose AES and DES are most commonly used cryptographic algorithms. Cryptography plays vital role in the security to maintain the confidentiality, authentication, integrity and non-repudiation of the information; and the encryption is the backbone of cryptography. Some significant issues in encryption have been discussed in this paper like simulation time, memory usage for performance estimation of DES and AES algorithms. In financial application encryption is done by DES but Memory usage in DES is more than in AES and AES provides the improvement in security level in information world as compared DES. In [1] authors presents a design of data encryption and decryption in a network environment using RSA algorithm with a specific message block size. The algorithm allows a message sender to generate a public keys to encrypt the message and the receiver is sent a generated private key using a secured database. An incorrect private

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

key will still decrypt the encrypted message but to a form different from the original message. Therefore, when an eavesdropper breaks in, it will return a meaningless message. In [3] authors implemented three encrypt techniques like AES, DES and RSA algorithms and compared their performance of encrypt techniques based on the analysis of its stimulated time at the time of encryption and decryption, it was concluded that AES algorithm consumes least encryption and RSA consume longest encryption time. We also observed that Decryption of AES algorithm is better than other algorithms. From the simulation result, we evaluated that AES algorithm is much better than DES and RSA algorithm. In[4]authors implement Asymmetric cryptographic algorithms that are a robust technology used to reduce security threats in the transmission of messages on the network. Nowadays, one of the disadvantages are the mathematical solutions because they require a greater amount of calculation that leads to the need for increased use of computational resources. This paper aims to optimize the RSA encryption algorithm and thus improve the security, integrity and availability of information. The results show the efficiency and functionality of the RSA algorithm in terms of information security.

II. PROPOSED SYSTEM

A)AES

AES is the acronym of Advanced Encryption Standard is a symmetric encryption algorithm processing data in block of 128 bits. AES is symmetric since the same key is used for encryption and the reverse transformation, decryption. The only secret necessary to keep for security is the key. AES may configured to use different key-lengths, the standard defines 3 lengths and the resulting algorithms are named AES-128, AES-192 and AES-256 respectively to indicate the length in bits of the key. Based on the key size the number of rounds varies, for 128,192and256 bits the number of rounds are 10, 12 and for 14 respectively. The older standard, DES or Data Encryption Standard.DES is up to 56bits only. To overcome the disadvantages of DES algorithm, the new standard is AES algorithm. This standard explicitly defines the allowed values for the key length (Nk), block size (Nb), and number of rounds (Nr). For the AES algorithm, the length of the input block, the output block and the State is 128 bits. This is represented by Nb = 4, which reflects the number of 32-bit words (number of columns) in the State.

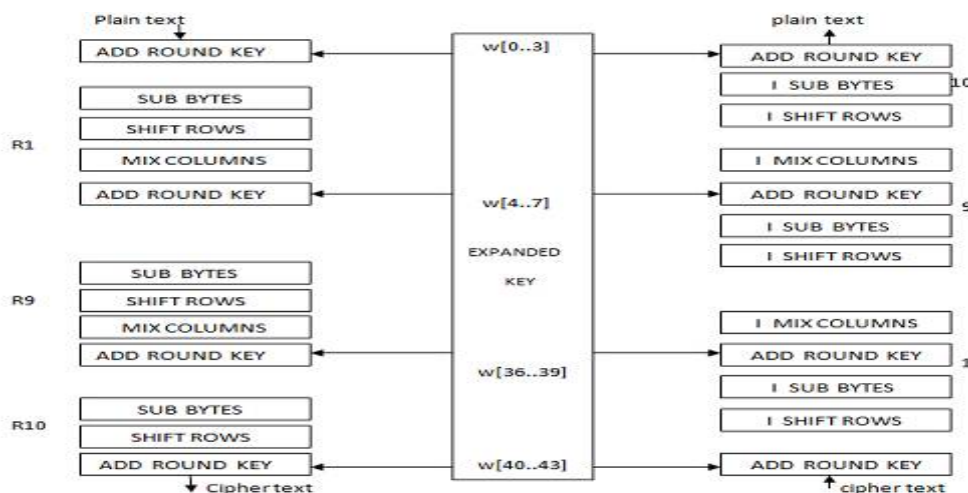


Fig 1: General structure of AES algorithm

AES Encryption : In encryption mode for a 128 bit key, the initial key is added to the input value at the very beginning, which is called an Initial Round. This is followed by 9 iterations of a normal round and ends with a slightly modified final round, as one can see in Figure 2. During one normal round the following operations are performed in

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirce.com

Vol. 5, Issue 5, May 2017

the following order: Sub Bytes, Shift Rows, Mix Columns, and Add Round key. The final round is a normal round without the Mix Columns stage.

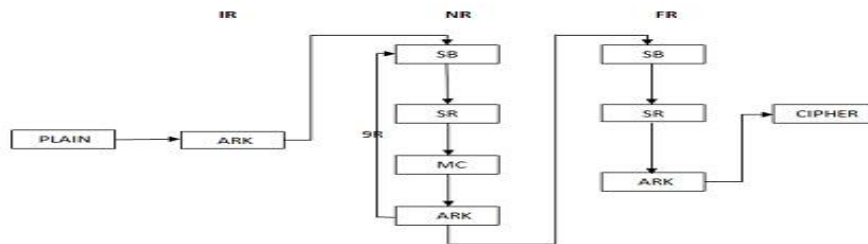


Fig 2: General structure of Encryption.

Steps in AES Encryption :

Step 1: Sub Bytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.

Step 2: Shift Rows—a transposition step where each row of the state is shifted cyclically a certain number of steps.

Step 3: Mix Columns—a mixing operation which operates on the columns of the state, combining the four bytes in each column

Step 4: Add Round Key—each byte of the state is combined with the round key; each round key is derived from the cipher key using a key schedule

B)RSA

RSA algorithm is asymmetric cryptography algorithm, which is named after the inventors **Rivest, Adi Shamir, and Leonard Adleman**. Asymmetric actually means that it works on two different keys i.e. **Public Key** and **Private Key**. As the name describes that the Public Key is given to everyone and Private key is kept private.

It is the first algorithm that can be used both for data encryption and digital signatures RSA algorithm's security depends on the difficulty of decomposition of large numbers. In the algorithm, two large prime numbers are used for constructing the public key and the private-key. It is estimated that the difficulty of guessing the plaintext from signal key and the cipher text equals to that decomposition of the product of two large prime numbers. So if somebody can factorize the large number, the private key is compromised. Therefore encryption strength totally lies on the key size and if we double or triple the key size, the strength of encryption increases exponentially. RSA keys can be typically 1024 or 2048 bits long, but experts believe that 1024 bit keys could be broken in the near future. But till now it seems to be an infeasible task.

To create an RSA public and private key pair, the following steps can be used:

Step 1: Choose two relatively large prime numbers, p and q . From these numbers you can calculate the modulus, $n=p*q$

Step 2: Select a third number e , which is an encryption key that is relatively prime to the product $(p-1)(q-1)$

Step 3: Calculate an integer d , which is a decryption key from the formula $e*d*mod(p-1)*(q-1)=1$

Step 4: The public key is the number pair (e, n) and the private key is the number pair (d, n) . Where the public key is known to the sender and receiver and the private key is known only to the receiver

Step 5: To encrypt a message, M , with the public key, creates the cipher-text, C , using the equation $C=M^e*modn$

Step 6: The receiver then decrypts the cipher-text with the private key using the equation: $M=C^d*modn$

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

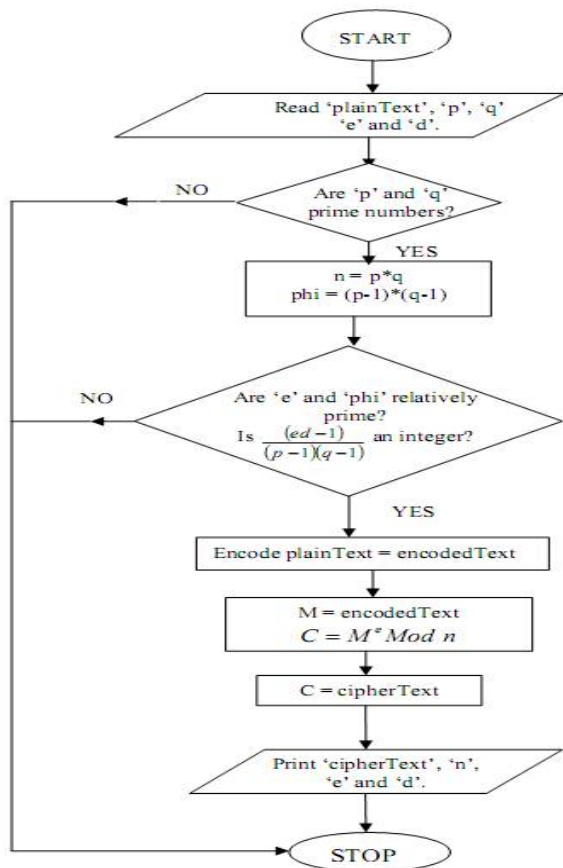


Fig 3a: Flowchart for RSA encryption

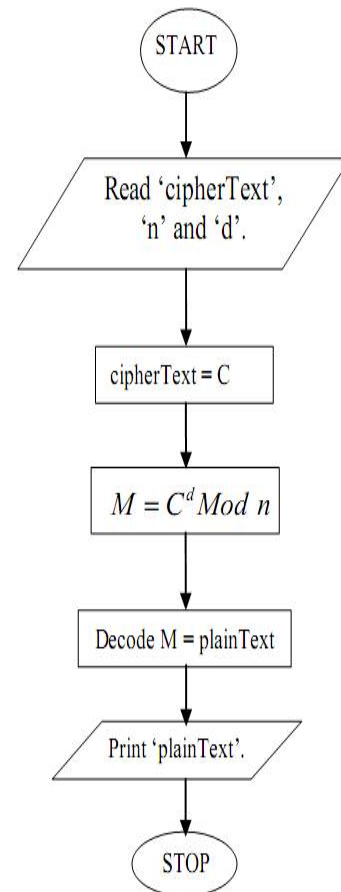


Fig 3b: Flowchart for RSA decryption

In this paper we have considered the combination of both AES and RSA algorithm to implement a hybrid cryptosystem having three modules as follows a) User module. b) Encryption module and c) Decryption module.

a) **The user module** is used to view two options Encryption and Decryption. The options are selected depends upon the user. If user wants to encrypt the file select the encryption option. Otherwise select the decryption option.

b) **The Encryption Module** is used to encrypt the text. First of all select the encryption option and then enter the plain text to be encrypted.

c) **The Decryption Module** is used to decrypt the cipher text easily. Select the decryption option to decode the encrypted message.

A plain text is taken as input from the user which is stored in the input file, this is encrypted using AES encryption algorithm for which a key creator program generates or loads the AES key or the sender private key. Once the message has been encrypted digital signature is used to provide authentication such that the receiver knows the message has arrived from the intended sender itself.

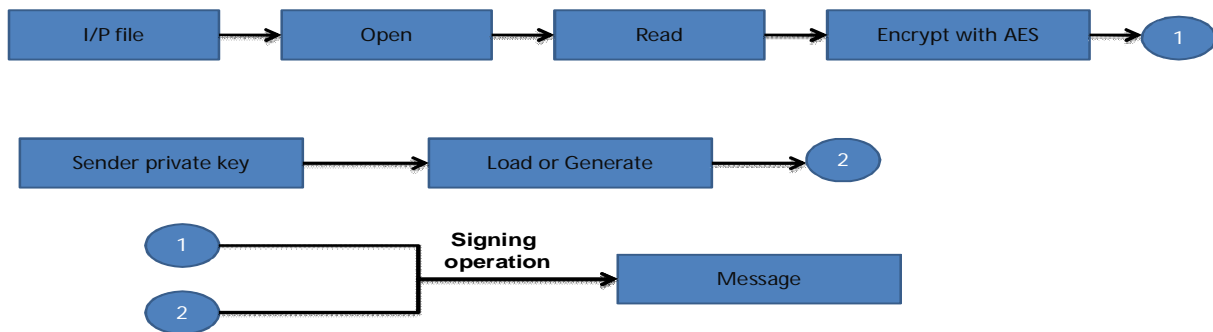
International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirccce.com

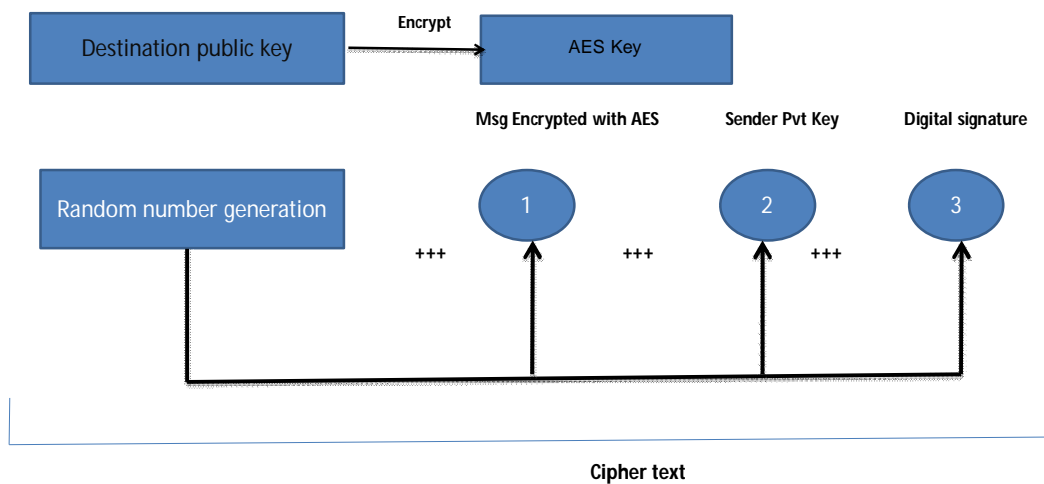
Vol. 5, Issue 5, May 2017

Level 1:



Further the AES key that was used for encryption will be encrypted again using asymmetric encryption or the RSA algorithm where the destination public key is used to encrypt only the AES key and not the message . On reaching this stage a combination of four parts i.e. the random number (generated using random number function in python) ,the encrypted message, the sender private key and the digital signature together will provide the cipher text.

Level 2:



On the receiving end, the cipher text will be detected and split operation is performed on it such the 4 parts i.e. the random number, the encrypted message, the sender private key and the digital signature are retrieved . Firstly the signature will be verified with the help of sender public key once authenticated next step is to retrieve the AES key that has been encrypted with destination public key to decode this the destination private key is used .On decrypting the

International Journal of Innovative Research in Computer and Communication Engineering

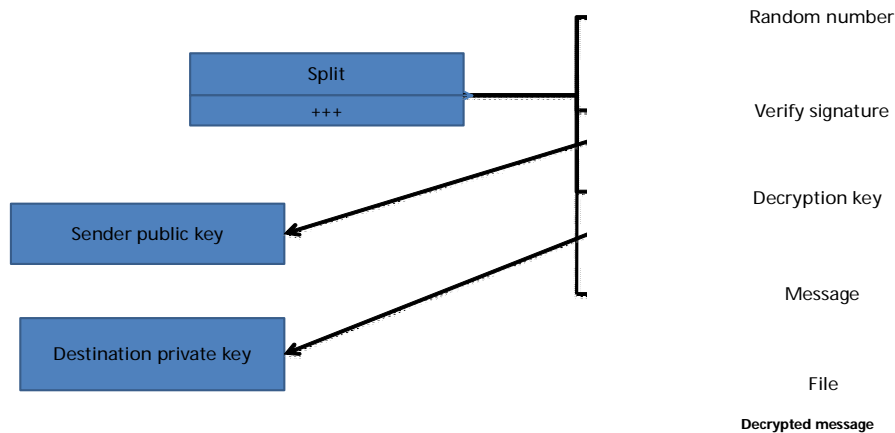
(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

AES key the encrypted text can be decoded using the same symmetric key this is the final stage where the original message is obtained.

Level 3



The system architecture provides the overview of data security for the complete processing of data transmission over internet or public network. The data or plain text is received from the sender from a Data source i.e. original data, on taking this as input it will enable AES encryption and the key used for encrypting the message will further be encoded using RSA algorithm. The encrypted key along with the encrypted message together as cipher will be transmitted to the receiver where the first level of decoding is done with the help of RSA decryption, with this being performed along with the authentication further the secret key will be made available as a result. Using this secret key or AES key the AES decryption is performed to decode the encrypted data and the original message is retrieved and directed to data destination.

The system architecture along with the architectural diagram is given below:

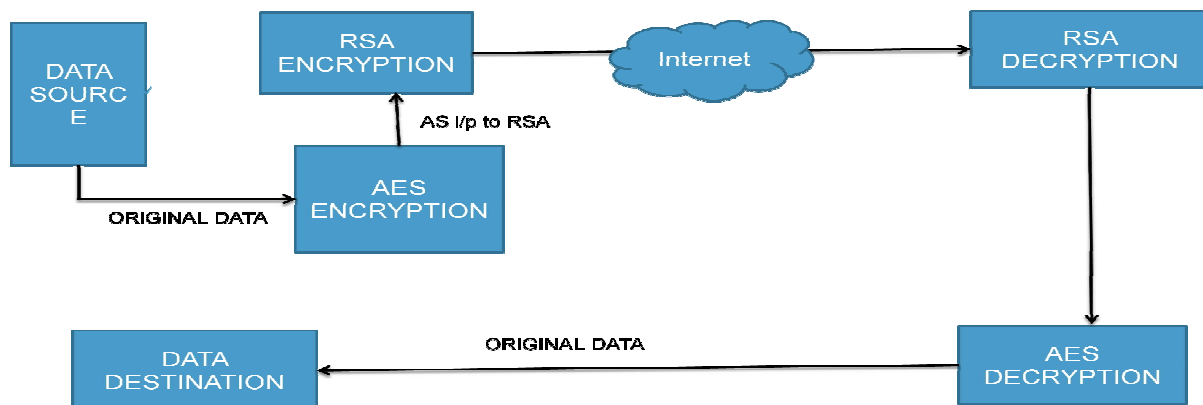


Fig 4: System Architecture

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

III. SIMULATION AND RESULTS

In order to implement the hybrid encryption technique python script is used and with the help of command prompt we execute the commands to run the program.

STEP 1:Open the command prompt and Run pythonfile with a .py extension

```

Applications Places System
x □ -
File Edit View Search Terminal Help
[aghora@parrot] ~/Desktop/Secure Email Encryption
$python test.py

```

STEP 2:A message “Enter e to encrypt and d to the decrypt.” is displayed.

Enter the appropriate option ‘e’ or ‘d’ to perform encryption or decryption respectively.

Option ‘e’ is selected for encryption.

```

Applications Places System
x □ -
File Edit View Search Terminal Help
[aghora@parrot] ~/Desktop/Secure Email Encryption
$python test.py
Enter e to encrypt and d to decrypt: e

Enter the message to encrypt:

```

STEP 3:A message “Enter the message to encrypt” Is displayed.

A sample message “hello world” is given.

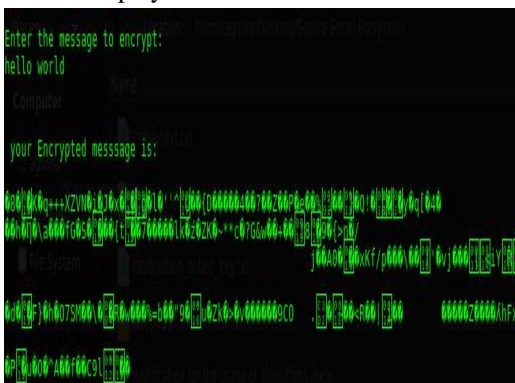
The encrypted message which is in unreadable form is displayed

```

Enter the message to encrypt:
hello world

Computer Name:
your Encrypted message is:

```



STEP 4:Run the .py file again and choose d to decrypt.

On execution the cipher is decoded to provide the original message “hello world”.

```

[aghora@parrot] ~/Desktop/Secure Email Encryption
$python test.py
Enter e to encrypt and d to decrypt: d

Your Decoded message is:
hello world

```

The proposed solution was feasible in encrypting and decrypting the data .The proposed solution be used for ensuring security and integrity while exchanging data between sender and receiver via email. While implementation it was observed that under normal circumstances hybrid encryption can be easily implemented and can be effectively used. Therefore it not only provides data security but also keeps up with the efficiency of the system.



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

IV. COMPARISON

The proposed system is more efficient with regard to existing techniques used for data security in email where PGP faces its issue with regard to compatibility, certification version, failed recovery of passwords and takes relatively more time to complete the process while hybrid crypto system with AES and RSA overcomes all the issues specified by the latter. AES by itself is prone to attacks if used alone and even RSA as a standalone system will take a lot of time to encrypt and decrypt data but with the hybrid system they overcome the drawbacks such that AES can encrypt large amount of data with great speed and will not be prone to attacks due to its encrypted key with RSA. Further RSA would not slower down since it only encrypts the key and not the entire cipher.

V. FUTURE ENHANCEMENTS

This project has its major focus on encrypting the rather than the entire cipher using asymmetric encryption. On providing a key that is large in size or if there is a need of encrypting a huge cipher it would get slower with RSA for which an optimized RSA algorithm can be used that would lower the memory, processor time and resource usage. Further even the AES algorithm can be strengthened by enabling dynamic permutation and substitution methods and also reducing the output data size by using some effective compression techniques.

REFERENCES

- [1] FaustoMeneses,WalterFuertes,JoseSancho,SantiagoSalvador,DanielaFlores,HernanAules,Fidel Castro, " RSA Encryption Algorithm Optimization to improve Performance and Security Level of Network Messages.", J CNS International Journal of Computer Science and Network security,VOL.16 No.8,August 2016.
- [2] BawnaBhat , Abdul Wahid Ali, Apurva Gupta, "DES and AES Performance Evaluation", International Conference on Computing, Communication and Automation, 2015.
- [3] By Dr. PrernaMahajan &AbhishekSachdeva IITM, " A Study of Encryption Algorithms AES, DES and RSA for Security.", India Global Journal of Computer Science and Technology ,Network, Web & Security Volume 13 Issue 15 Version 1.0 Year 2013.
- [4]G.singh and A.Supriya,"A Study of encryption algorithms(RSA,DES,3DES AND AES) for Information Security" in International Journal of Computer Applications 67(19),2013.
- [5] Nentawe Y. Goshwe, Department of Electrical/ElectronicsEngineering ,University of Agriculture, "Data Encryption and Decryption Using RSA Algorithm in a Network Environment" , Makurdi IJCSNS International Journal of Computer Science and Network Security, VOL.13 No.7, July 2013 .
- [6] Prashanti.G, Deepthi.S&SandhyaRani.K. "A Novel Approach for Data Encryption StandardAlgorithm".International Journal of Engineering and AdvancedTechnology (IJEAT) ISSN: 2249 – 8958, Volume-2,Issue-5, June 2013.
- [7]Afolabi, A.O and E.R. Adagunodo, "Implementation of an Improved data encryption algorithm in a web based learning system.", International Journal of research and reviews in Computer Science, Vol. 3, No. 1,2012.
- [8] Akash Kumar Mandall, Chandra Parakash2 "Performance Evaluation of Cryptographic Algorithms: DES and AES", IEEE Students' Conference on Electrical, Electronics and Computer Science,2012.
- [9] Chehal Ritika, Singh Kuldeep. "Efficiency andSecurity of Data with Symmetric Encryption Algorithms". International Journal of AdvancedResearch in Computer Science and SoftwareEngineering, ISSN: 2277 128X , Volume 2, Issue 8,August 2012.
- [10] Gaurav, S., "Secure file transmission scheme based On hybrid encryption technique.", International Journal of management, IT and Engineering, Vol. 2, issue 1,2012.
- [11]Q.Liu, Y.Li,T.Li and L.Hao "The research of the batch RSA decryption performance" in journal of computational Information system 2011.
- [12]X. Zhou and X. Tang, "Research and implementation of RSA algorithm for encryption and decryption",in 6th International Forum on Strategic Technology(IFOST),2011.