IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

An Approach To Multi-Level Encryption

[1]Satyander, [2]Shalini Bhadola, [3]Kirti Bhatia

[1]M.Tech Student, [2]Assistant Professor, [3]Assistant Professor
Computer Science and Information Technology,
Sat Kabir Institute Of Technology & Management, Bahadurgarh, Haryana, India

Abstract : In this era, the most important thing for user as well as for an organization is network security where data of most of companies/organization is stored on clouds. So we must have to find a solution so that data must be safe during network transmission. In this regards most efficient way is to encrypt the data which we transmit from source to destination. Then at destination again decrypt the original data form encrypted data. Some of the data is more critical like some government data or military communication, banking transactions etc.. When data falls in wrong hand may leads to big devastating.

In this paper, a solution for above situation a multi-level encryption is given. In this multilevel encryption, data is more secure than the conventional encryption which involves multiple rounds of encryption with same or different keys and this make the algorithm complex and more powerful.

***Index Terms* - Cryptography, Encryption, Decryption, private-key, public-key, RSA, AES, Multilevel Encryption.**

I. Introduction

Data security is importance in present time as lots of information is being communicated via network. A suitable methodology for privacy transformation is best to make a data protected over network. Different methods are implemented in order to protect the sensitive data. Now a days most of the data is secured by the technique of encryption and certificates. Most of methods are based on cryptography technique.

Multi-level encryption is a new concept that is used for making the system more secure than existing cryptosystems. Multi-level encryption is the process of encrypting the plain text with one or more time with same of different no of keys. It makes the process more complex and powerful than existing.

II. CRYPTOGRAPHY AND TYPES

Cryptography: It is a technique to which information is send in a secure manner so that only authorized user is able to receive this information. It refers to the scrambling of the data and make it meaningless for the third party during transmission

There are three basic components of cryptography system

- **Plain text** : Source / information/data / original message
- **Key** : Necessary for encryption process.
- **Cypher text** : Unrecognized data /encrypted data / encrypted message

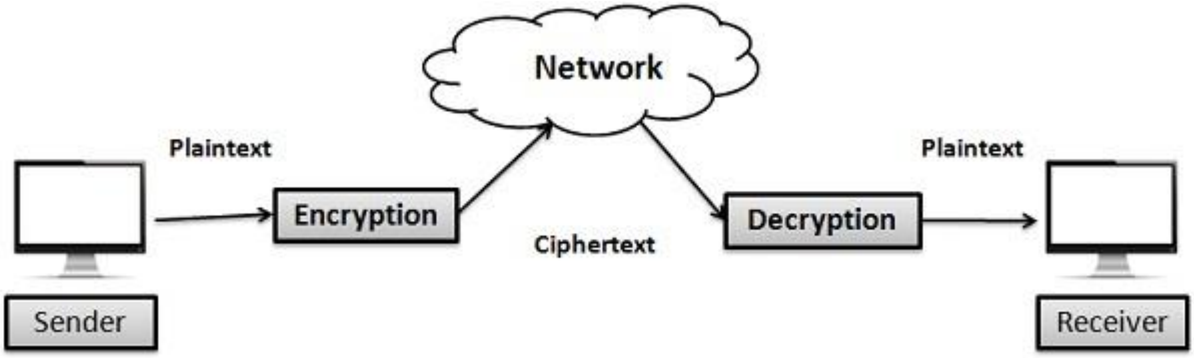


Fig 1: Encryption Decryption Process

The original text is encoded with encryption algorithm. This process called as encryption. The reverse process to get back the encrypted data into plain text by using decryption algorithm. This process is called decryption. Decryption process is the reverse of encryption.

Objectives of cryptography are:

- **Confidentiality :** Confidentiality means to the keep information secret / private.
- **Data integrity :** It ensure accuracy and consistency (validity) of data over its lifetime.

- **Authentication :** It ensure that data is genuine and verified at any stage and completely trustworthy.

Of course, the algorithm requires the key to be kept secret or long enough so that it takes even longer to break. For example, a 40-bit key has one trillion combinations whereas a 128-bit key has 3.4*1026 trillion combinations [1]. There are two types of key-based algorithms i.e Symmetric and Asymmetric.

Symmetric Key Algorithms, also known as private-key / conventional / secret-key algorithm. It require that sender and receiver uses a single key before they start communicate securely. In this type of algorithms, the encryption key used for encryption and the decryption key used for decryption are the same and security of information depends on the degree of key secrecy from the unauthorized user / intruders.

During the transmission key must remain secret. Encryption process can be done like $\text{ENCRYPTION}_{\text{KEY}}$(MESSAGE) = CIPHER TEXT and Decryption processes as: $\text{DECRYPTION}_{\text{KEY}}$(CYPHER TEXT) = MESSAGE respectively. This method is extremely fast and efficient. It also provides integrity and confidentiality. But it fails to provide authentication. [2][3][4].

Asymmetric key algorithm, also known as public-key algorithms which operate with public encryption key and private decryption key. Encryption key is made public and any sender can use the key to encrypt the message, but only a authorized user can use the private key (decryption key) to decrypt the ciphertext. There are some example which are based on this type of algorithms like RSA, Rabin and Elgamal [1][2][4]. Asymmetric algorithms are hard to implement and require significant processing power due to fundamental mathematical operations such as modulus. In this paper we will talk about the AES and RSA algorithm and their implementation in multilevel security layers which will be fast and as much more secure than existing AES and RSA.

Proposed Multi-level encryption can work better compared to single encryption. Multi-level encryption involved the encryption of a message single or multiple times by using one algorithm with same key or same algorithms with different keys or by using different algorithms[13]. But the proposed algorithm works faster and provide extra security to data in an efficient manner. Not all algorithm with multiple computations are always better but an efficient algorithm can provide same layer of security in faster way.

AES(Advanced encryption standard) this is a symmetric block cipher algorithm that encrypt and decrypt data. It is fast unlike its predecessor DES. AES has a minimum block size of 128 bits. This algorithm used the encryption keys of different sizes 128 ,192 ,256 bits for encrypting the data also uses the same key size for decrypting the data of 128 bits of block size. There are a number of parameters which are depend on the key length in AES. Assume that if the key size used for the algorithm is 128 bits then 10 number of rounds will be used for the data encryption. Similarlarly if key size is of 192 bits then no of round will be 12 same 14 no of rounds for 256 bits of key size. Most commonly key size used for AES encryption is 256 bits.

AES is based on 'substitution permutation network' . So we used a sequence of linked operation some of which are substitution and some are permutations. These number of steps used in the transformation operations is a round sequence of operations that convert the input plaintext into the final cipher text (output). These no of rounds consist some steps which are Shift Rows, Round Key, Substitute Bytes and Mix Columns. These steps depend on the encryption key. These set of rounds are applied in reverse order to get the original plaintext form the cipher text. These round sequence uses the same encryption key which is used to encrypt the plaintext.[7].

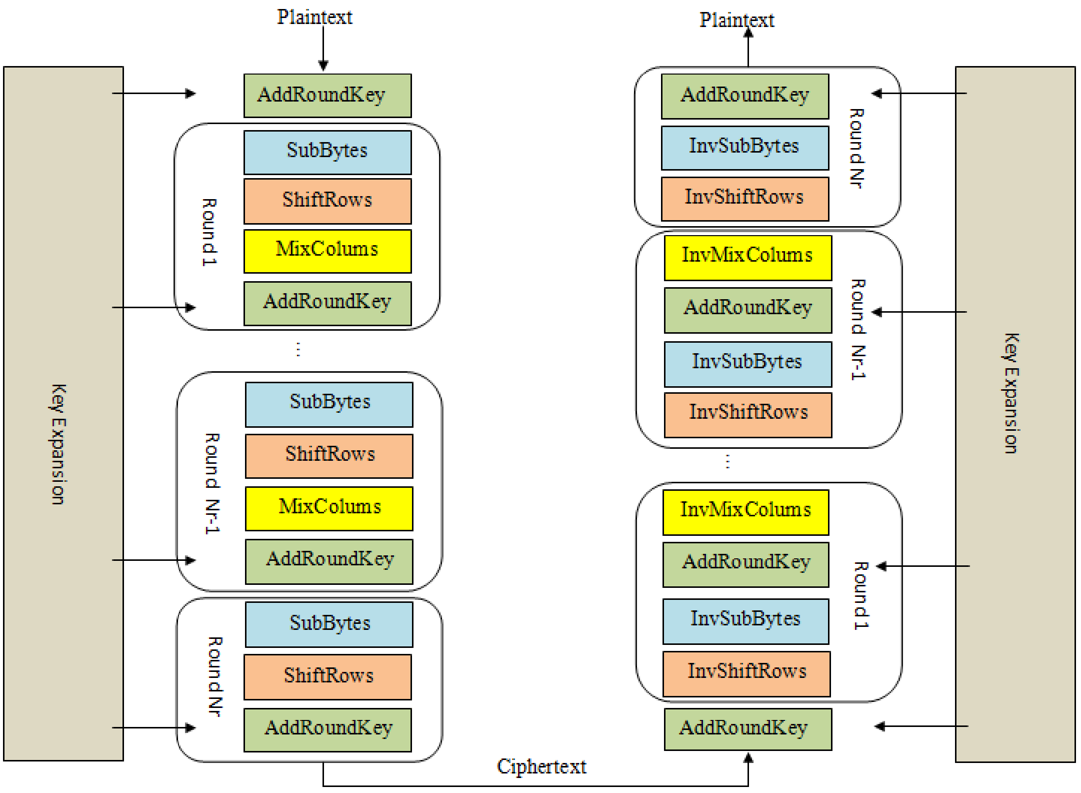


Fig 2: AES Encryption Decryption Process

The number of rounds varies for the 128, 192, and 256-bit variants (10, 12, and 14 rounds respectively). The key schedule is different for each variant.

In rijndael, byte is the basic unit for ciper operation. These bytes are finite field of elements which are represented as polynomial expression,

$$b_7x^7 + b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x + b_0 = \sum_{n=1}^{7} b_i x^i$$

Here, these bytes with bits b0, b1...... b7 represents the finite field elements. Some Finite field operations such as addition, multiplication are important for key scheduling and rounding function. These finite field elements can be added by adding th co-efficient of corresponding power in their polynomial representation. Addition of these group can be performed in GF(2), such that modulo 2 is 1+1=0.

The input key provided is expended as an array of 44 32 bits w[i]. Random four word are used as a round key for each round of encryption.

The four sub-operations of AES, one for permutation (Shift Rows) and three of substitution (Add Round Key, Substitute Bytes, , and Mix Columns) [7]. These sub-operations are explained here.

Add Round Key : The Add Round Key is the only phase of this AES algorithm that operate directly on the round key. Here in this, the input to the round is Ex-OR with round key. If this round is the last round then output produced is the cipher text. If the round is not the last round then begin another similar round till the last round.

Substitute Bytes : In substitution phase of AES, we split the input into bytes and passes each byte through S-Box. AES uses the same S-Box for all bytes. These input bytes are picked by checking the same S-box table and the result will comes in the form of a matrix of 4 rows and 4 columns.

Shift Rows : In Shift rows, a shift operation is performed and the all the 4 rows are shifted to the left. If there is any entry which left off, will be reinserted on the right side of rows in matrix. Theses shift are performed on each row in a manner such thst if first row is not shifted, Second row is shifted one position to left and so on. The result will be a matrix consisting of same size but in shifted positions.

Mix Columns : In mix columns, here the columns of matrix of 4 byte is transformed by using some special mathematical functions which takes the input as 4 byte of one columns and transform into the output of columns in an new bytes. This output result is another new matrix consisting of 16 new bytes. This site is not performed in the last round[8].

RSA(Advanced encryption standard)

RSA algorithm was developed by Ron Rivest, Adi Shamir and Leonard Adleman in 1977 at MIT. RSA is an asymmetric key algorithm. The Rivest-Shamir-Adleman (RSA) cryptosystem most widely accepted and implemented general-purpose approach to public-key cryptography. It uses different keys for encryption and decryption. RSA (a public-key cryptography), involves a public key and a private key. The public key can be used to encrypt messages/data by everyone. Messages/data encrypted with the public key can only be decrypted using the private key.

. The RSA algorithm involves three basic steps.

1. **Key Generation :**

   RSA algorithm uses asymmetric approach i.e public key and private key. Public key is used for encrypting the plain text into cipher text and private key is used for decrypting the cipher text into plain text. There are few steps for key generation :

   a. Assume 2 large prime no P and Q.
   b. Compute N by using the given formula i.e N = P * Q
   c. Compute Phi (N): $\phi(n) =$ (P-1) * (Q-1) , $\phi(n)$ is Euler's totient.
   d. Choose the public key exponent e such that 1 < e < $\phi(n)$ and e, $\phi(n)$ are co-prime i.e. GCD (e, $\phi(n)$) = 1
   e. Determine private key exponent d such that d * e= 1 * mod ($\phi(n)$) , d is the multiplicative inverse of e^{-1} mod ($\phi(n)$)
      Public Key: (n, e)
      Private Key: (n, d)

2. **Encryption:**

Plaintext :	$M < n$	Plain text should be less than product of prime numbers.
Ciphertext :	$C = M^e (\text{mod } n)$	This is the resultant cipher text.

3. **Decryption :**

Ciphertext :	C	This is the cipher text
Plaintext :	$M = C^d$ (mod n)	Calculation of plain text from the ciper text.

The RSA is most widely used algorithm because it allows public key for encryption process and the private key for decryption. It ensure confidentiality, integrity, authenticity and non-reputability of data. It is important to note that a weak key generation will make RSA very vulnerable to attacks. Therefore two large random prime numbers are used to calculate the public key and the private key.. The RSA algorithm becomes effectiveness from the fact that it's difficult to compute factors. Multiplication of two primes is easy but performing the reverse operation to form exact factors is so difficult. It became harder if the values of p and q are large. As the key length of modulus becomes large, it takes enormous time to get the factors. The challenge of RSA factoring was a big problem for researcher into computational number theory to recover RSA keys in a definite time. RSA100 was affected by April 1 1991, But many numbers are still not factored and expected to remain un-factored for some time. However, At later some researcher's tries to crack the RSA Keys in polynomial- time. Most popular algorithm was given by Shor in 1994. It is a quantum computer algorithm which can be used for integer factorisation. But till now only factor of 21 is possible to break on quantum computers because of its qubits requirement. So no quantum computer is built till date which can recover RSA factors.

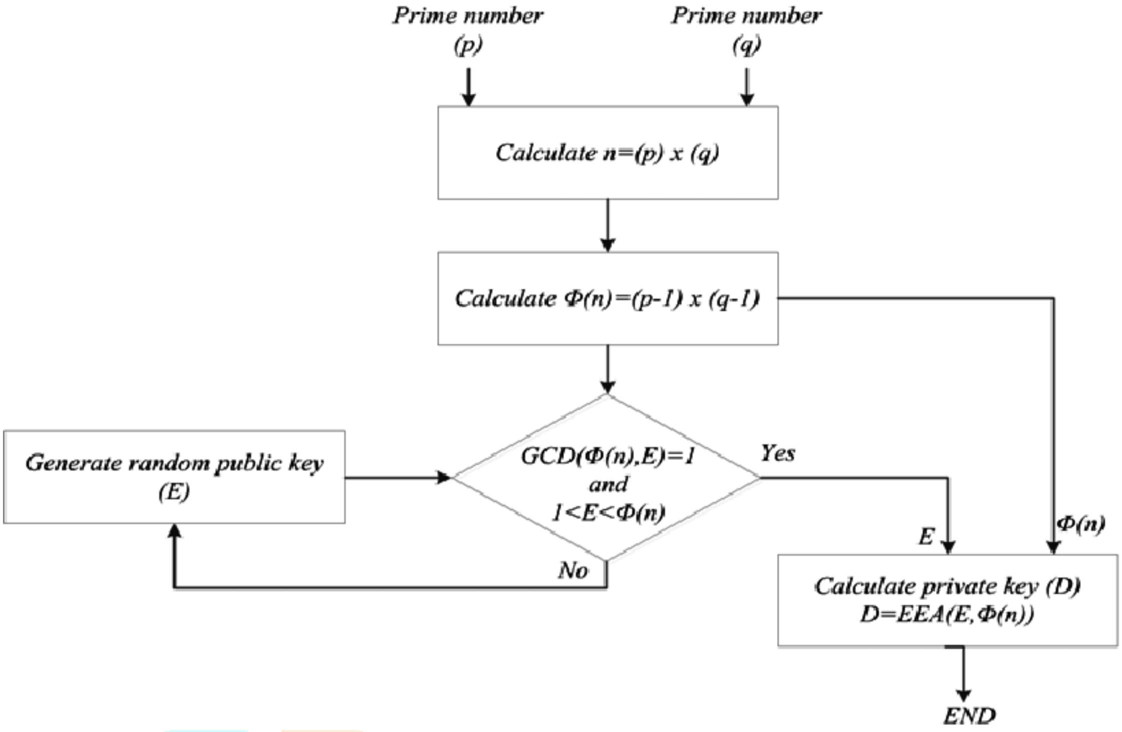

Prime number (p)
Prime number (q)
Calculate n=(p) x (q)
Calculate Φ(n)=(p-1) x (q-1)
Generate random public key (E)
GCD(Φ(n),E)=1 and 1<E<Φ(n)
Yes
No
E
Φ(n)
Calculate private key (D) D=EEA(E,Φ(n))
END

Fig 3: RSA Encryption Decryption

III. Related Work and Implementations

The idea of combining the approach of RSA and AES is being used for both symmetric and asymmetric encryption is not a new approach. Security is always a prime issue for purchase researchers and experimenters. There are some implementations done by researchers using hybrid approach as well as multi level cryptography approach.

Security in 2016 includes multiple phases to be applied on the data namely RSA, DES, hybrid algorithm. The keys that were used in the last step were string modulus, private, public and integer key [9].

Another approach was combining a symmetric and public key method in 2012 hair where used for encryption was used for key exchange. It also consists of pseudo random number generation unit for key generation process and GCD computing unit in the RSA algorithm [10].

Multilevel encryption is found in 3DS, AES provides cryptographic assurance of message integrity. Multiphase or multi level encryption technique uses plain text (message) to encrypt in single or multi level(k times) encryption with the same or different keys. Results in improved security to overall system.[11]

IV. Proposed Solution

This type of encryption scheme is more effective than a single encryption scheme. In this encryption scheme, more the number of rounds, more security due to different keys used in each round of encryption. In cryptography, more data complexity in encryption technique used for data security , it enhances the security during transmission and store in a system. A subsequent increase in round of encrypted data will increase the data encryption complexity enormously, and also leads to complications in data decryption.

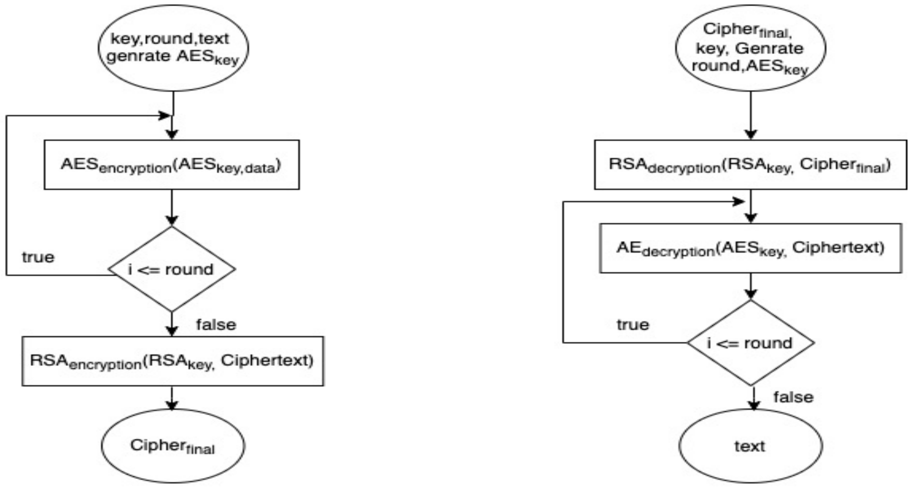
Here, in the type of purposed solution we use a round function which is used to provide a layered security to the data. For AES encryption the AES key is not directly used as used in the AES encryption which also enhance the AES key security. In each round of data encryption a subsequent cipher text is generated and encrypted till the round function. Then the cipher is encrusted with RSA security with a public and private key mechanism which enhance the security of the encrypted data. The same process is followed in case of decryption. If due to any circumstances a unauthenticated user will able to decrypt the data then it is not get the final text after breaking single layer of security.

```
Algorithm for encrypting data with Multilevel encryption approach
    Step 1 : Generate 2 prime no x and y
        x used as a Key to encrypt where y used for no of rounds.
    Step 2 : Choose $AES_{key}$ = x*y
    Step 3 : Encrypt data with $AES_{key}$ till y rounds. find ciphertext.
    Step 4 : Encrypt the ciphertext with RSA with Public key and get $Cipher_{final}$.
```

```
Algorithm for decrypting data with Multilevel encryption approach.
    Step 1 : Decrypt the $Cipher_{final}$ with Private key with RSA. find ciphertext.
    Step 2 : Calculate round y from key and $AES_{key}$.
    Step 3 : Decrypt the data with $AES_{key}$ till y rounds.
    Step 4: Find plaintext.
```

Fig 3: Multi-level Encryption Decryption

Example for encryption with multilevel Encryption aproach.


key,round,text genrate AES$_{key}$
AES$_{encryption}$(AES$_{key,data}$)
true
i <= round
false
RSA$_{encryption}$(RSA$_{key,}$ Ciphertext)
Cipher$_{final}$
Cipher$_{final,}$ key, Genrate round,AES$_{key}$
RSA$_{decryption}$(RSA$_{key,}$ Cipher$_{final}$)
AE$_{decryption}$(AES$_{key,}$ Ciphertext)
true
i <= round
false
text

Multilevel Encryption

Multilevel Decryption

Lets take an example

```
Enter no of rounds between (1 - 1500) to encrypt data: 5
Enter a no to encrypt with AES : 12823105746930315101

KEY     : 4000557202740409
AES KEY : 20002786013702045
Encrypted on 1 round : 7099139665151472948
Encrypted on 2 round : 16860710063976609505
Encrypted on 3 round : 7307050261630191216
Encrypted on 4 round : 9813939479609809507
Encrypted on 5 round : 3311061768697571000
RSA Encrypted Text:
2032016345144915914184712473045157424753585211506475130932576005074296609522017764986880030845567074759793817
312546820769944429619615429406101254978297553

RSA Decrypted Text : 3311061768697571000
Decrypted on 1 round : 9813939479609809507
Decrypted on 2 round : 7307050261630191216
Decrypted on 3 round : 16860710063976609505
Decrypted on 4 round : 7099139665151472948
Decrypted on 5 round : 12823105746930315101
```

Here the illustrated example has been explained to clear the idea of multilevel encryption algorithm. The encryption round can be n number to enhance the security of the data.

V. Conclusion

Multiple encryption is used for better security with the help of different combination of multiple algorithms. In multiple / multi-level encryption, if some cipher are broken still it ensures the confidentiality of data which can be maintained by multiple encryptions. In multi-level encryption its primary task is to provide security as well as confidentiality of data. Case study of different type of multilevel encryption gives the idea and positive aspect toward a new hybrid approach. it also maintain the standard for network security also can be used in different ways like password protection for any application. implementation of these type of algorithms can be used in the field of technology, banking, defence, government officials website for ensuring security.

Multilevel data encryption is a technique which ensures the secrecy and privacy of data and information. it creates complexity in data encryption algorithm due to multiple operations. These operations can be in single phase or multiple phase. These operation can be encrypted with single key or multiple keys during each round of encryption and provide enormous complexity in data encryption.

VI. FUTURE SCOPE

Now a days a large no of attacks increases needs for secure communications. So a more secured cryptographic algorithm needs to be proposed and implemented. The multi-level encryption can be widely used in most of the applications. Here the round function is used to avoid the risk of AES software. Future work will focus on investigating and implementing a countermeasure against the multilevel implementations and their performance. Also try to prevent vulnerabilities attacks and develop more secure system.

VII. References

[1] J. E. Soric, "*Cryptography Honors Project*," http://cs.bluffton.edu/~jsorice/projects/cryptography.

[2] Bruce Schneier, *Applied Cryptography*, 2nd ed., John Wiley and Sons, Inc. 2001.

[3] Paul C. Van Oorschot, and Scott A. Vanstone, Alfred J. Menezes, *Handbook of Applied Cryptography*, CRC Press 1997.

[4] Harry Katzan Jr., *The Standard Data Encryption Algorithm*, Petrocelli Books, 1997.

[5] Himanshu Gupta, Vinod Kumar Sharma, "*Multiphase Encryption: A New Concept in Modern Cryptography*", IJCTE, Vol 05, No 4, 2013.

[6] Shashikant Kuswaha, Praful B. Choudhary, Sachin Waghmare, Nilesh Patil," *Data Transmission using AES-RSA Based Hybrid Security Algorithms*" IJRITCC, Vol 3, No 4, 2015

[7] Zhang Hanli Zhaohui, Yuan Kun, "*An Improved AES algorithm based on chaos*", Multimedia Information Networking and Security, International conference 2009.

[8] Aida Janadi, "*AES immunity Enhancement against algebraic attacks by using dynamic S-Boxes*", ICTTA 2008.

[9] Smita Chourasia, Kedar Nath Singh "*Information Systems Design and Intelligent Applications*" Springer, New Delhi, 2016

[10] Farhan Abdul-Aziz Khan, Adnan Abdul-Aziz Gutub, "*Hybrid Crypto Hardware Utilizing Symmetric-Key and Public-Key Cryptosystems*" International Conference on Advanced Computer Science Applications and Technologies – ACSAT2012 .

[11] Himanshu Gupta and Vinod Kumar Sharma "*Multiphase Encryption: A New Concept in Modern Cryptography*" IJCTE, Volume 5, Number 4, August 2013.

[12] W. Diffie and M. Hellman, "New directions in cryptography", IEEE Transactions on Information Theory,Volume 22 , Issue: 6 , November 1976

[13] Rivest, R. L., Shamir, A., Adelmann, L.: "*A method for obtaining digital signature and public –key cryptosystems*", Commun. ACM, 1978, VOL. 21, pp. 120-126.

[14] Chourasia S., Singh K.N.," *An Efficient Hybrid Encryption Technique Based on DES and RSA for Textual Data*". In: Satapathy S., Mandal J., Udgata S., Bhateja V. (eds) Information Systems Design and Intelligent Applications. Advances in Intelligent Systems and Computing, vol 433. Springer, New Delhi.

[15] Kaur, Khushdeep, and Er Seema. "*Hybrid Algorithm with DSA, RSA and MD5 Encryption Algorithm for wireless devices*" IJERA, 2.5 (2012): 914-917

[16] H.M. Sun, M.E. Wu, W.C. Ting, and M.J. Hinck, "*Dual RSA and its Security Analysis"*, IEEE Trans. On Information Theory, vol.53, no.8, pp. 2922-2933, August 2007.

[17] H. M. Sun, M.J. Hinek, and M.-E. Wu, "*On the design of Rebalanced-RSA, revised version of Centre for Applied Cryptographic Research*", Technical Report CACR 2005-35, 2005.

[18] Wang Rui; Chen Ju; Duan Guangwen, "*A k-RSA algorithm*," ICCSN, 2011 IEEE 3rd International Conference on, vol., no., pp.21, 24, 27-29 May 2011