A REVIEW ON MULTI-LEVEL ENCRYPTION

[1]Khaitul Abeez,
Student, Department of Electronics and Communication Engineering, Swami Devi Dyal Institute of Engineering and Technology, Haryana, India

[2]Sandeep Sangwan,
Assistant Professor, Department of Electronics of Communication Engineering, Swami Devi Dyal Institute of Engineering and Technology, Haryana, India

[3]Majid Zaman
Scientist "D"
Directorate of IT and SS
University of Kashmir,
Srinagar, J&K

[4]Muheet Ahmed Butt
Scientist "D"
PG Department of Computer Sciences,
University of Kashmir,
Srinagar, J&K

ABSTRACT : The current era is all about data or information which is stored in computers, files etc. Some of this data may be extremely critical which one cannot afford to share with others. When data falls into wrong hands, the results can be devastating. In order to securely protect this data, encryption is needed so that no unwanted party may get access to it. Governments use it to protect classified data, businessmen use it to secure corporate secrets etc.
In this paper, an introduction of multi-level encryption is given by which the information is encrypted in a much secure manner as compared to the conventional methods of encryption as it involves various rounds of encryption and decryption which makes it complex.

I. INTRODUCTION

Information security is a challenging issue of data communications in todays technological world. There is a need for a stronger encryption algorithm which is very difficult to crack[4]. Different methods are employed in order to protect the sensitive data. Today most of the means of confidential data and code storage rely on using cryptographic schemes e.g. encryption or certificates. Therefore the important aspects of solid security systems are based on cryptography[3].
Multi level encryption is a new concept in the field of modern cryptography. Cryptography is the science of designing methods which allows the information to be sent in such a secure manner so that only the intended recipient is able to retrieve this information[13]. It refers to the scrambling of the contents of the data so as to make it meaningless for the third party during transmission. The basic principle of cryptography is as follows: The original message to be sent is known as plaintext. This message is then encoded using encryption algorithm. This process is called encryption. The encrypted message is called cipher text which is retrieved back into plaintext by the process of decryption. The process of decryption is reverse that of encryption.

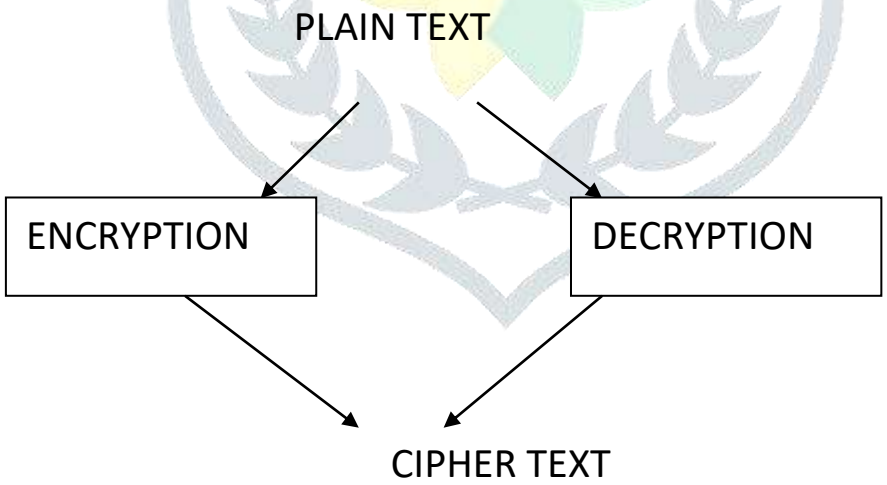


Fig: Block diagram of basic cryptography

Cryptography is used to achieve following objectives:

- Confidentiality: to make sure that the information remains private. Confidentiality is attained by using encryption.
- Data integrity: to ensure that the information is protected from accidental or intentional modification. Data integrity is achieved by message authentication codes or hashes. A hash value is derived from the data sequence. It is a fixed length numeric value. These are used to verify the integrity of data sent through insecure channels. The hash value of the data received is compared with the hash value of data sent to check for any alteration.
- Authentication: to ensure that the data originates from the desired party. Authentication is ensured by using digital certificates.

The field of information security has become a dynamic research area as the number of cyber attacks are increasing day by day. The conventional methods of encryption can only maintain the data security. The secret data can also be accessed by the unauthorised users for malicious purpose. Therefore it is essential to apply effective encryption/ decryption methods to improve data security[4]. Multi level encryption can be seen as a better option as compared to single encryption. Multi level encryption involved the encryption of an already encrypted message one or more times by using same algorithm with same key or same algorithms with different keys or by using different algorithms[13]. The choice depends on the application used. Since the multi level encrypted cipher text requires multiple computations therefore the cryptanalysis involved is much difficult as it requires more time and efforts. This means the multi level encrypted cipher text is much secure.

There are two types of encryption algorithms: Symmetric and Asymmetric

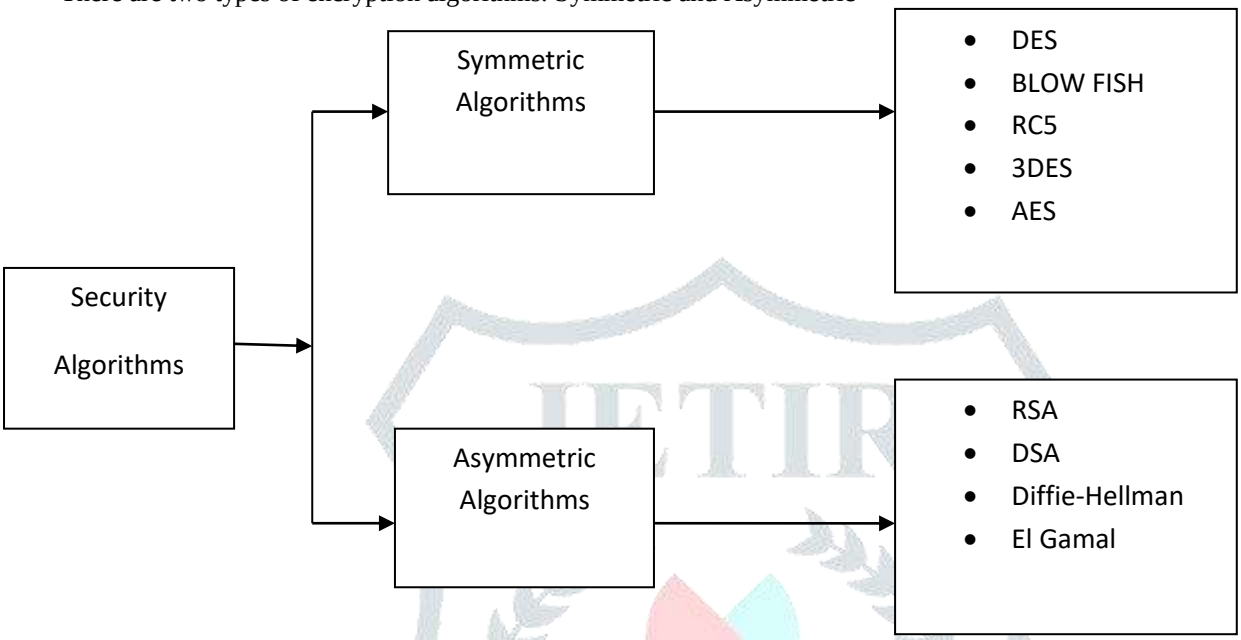


Fig : Diagram showing various encryption algorithms

Symmetric key algorithm: In symmetric key algorithm, same algorithm and same key is used for encryption and decryption. Private key is used at both the ends to encrypt and decrypt the message. This method is extremely fast and efficient and it also provides integrity and confidentiality. But it fails to provide authentication.

Asymmetric key algorithm: In asymmetric key algorithm, two keys are used one is the private key and the other is the public key. The encryption can be done by anyone using the public key but decryption can only be performed by the one carrying the private key[16].

DES(Data encryption standard): DES is an earlier used symmetric algorithm for encryption. DES takes a plain text of 64 bit cipher and generates a 64 bit cipher text at the encryption site. Again it takes a 64 bit cipher text and generates a 64 bit plain text at the decryption site. Both for encryption and decryption same 56 bit cipher key is used. The encryption process is made of two permutations (P-boxes) called as initial and final permutation, and sixteen Feistel rounds, Each round uses a different 48-bit round key generated from the cipher key according to a predefined algorithm[12].

The basic DES encryption operation can be represented as:
Ciphertext = S_K (Plaintext),
And double encryption is obtained as:
$C = SK_2 [SK_1 (P)]$

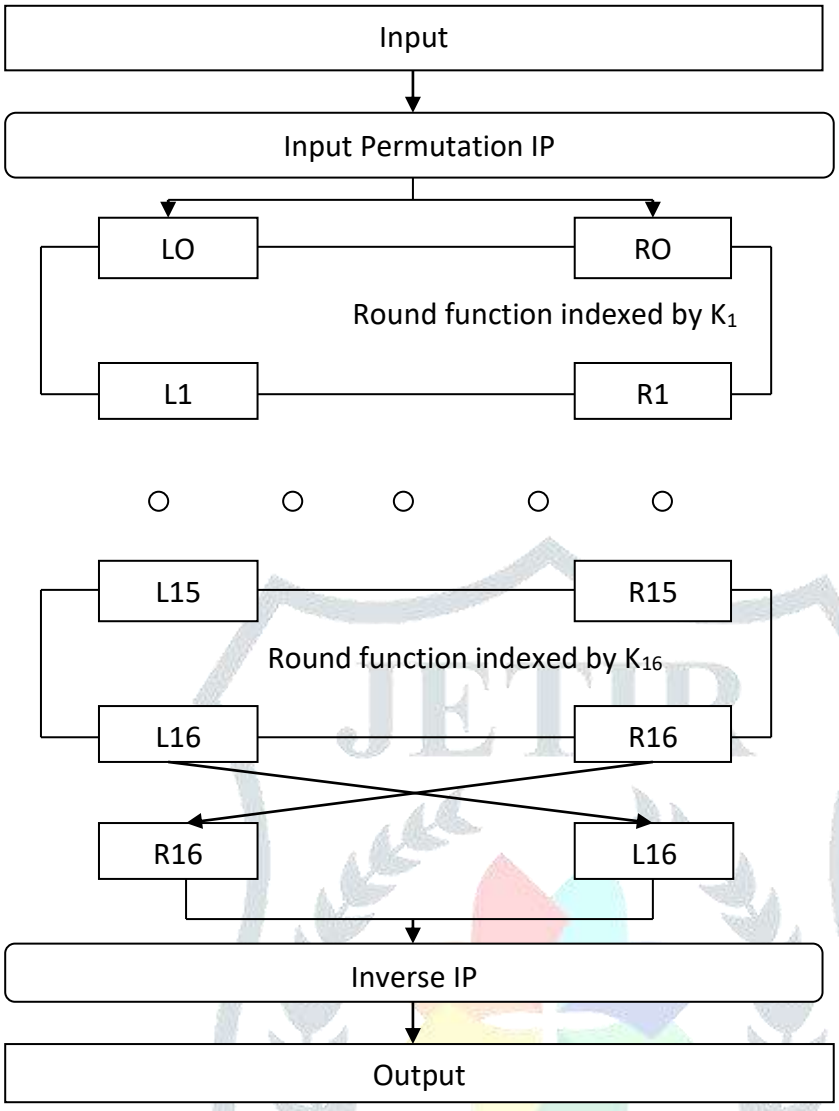


Fig. Encryption With DES

Triple DES (or 3DES): It is a common example of multiple encryption, which uses three DES keys as K1, K2 and K3 with the size of 56 bits. Each block of data is encrypted by different three 56-bit keys. The sender and receiver have to follow complex procedures to accomplish the encryption and decryption process in 3 levels. Also the large key size increases the complexity of algorithm. Moreover the keys are of fixed size and do not change with time.

The encryption algorithm can be stated as:

$C = EK_3(DK_2(EK_1(P)))$

i.e., DES encrypts with key K1, DES decrypts with key K2, and then DES encrypts with key K3.

Decryption is the reverse process as:

P = DK1(EK2(DK3(C)))

i.e., decrypt with key K3, encrypt with key K2, and then decrypt with key K1.

The triple encryption process takes place on the plaintext having size of 64 bits of data. In this technique, the middle operation is the reverse of the first and last operations. The strength of the algorithm improves when using a set of different keys instead of symmetric keys or same keys[13].

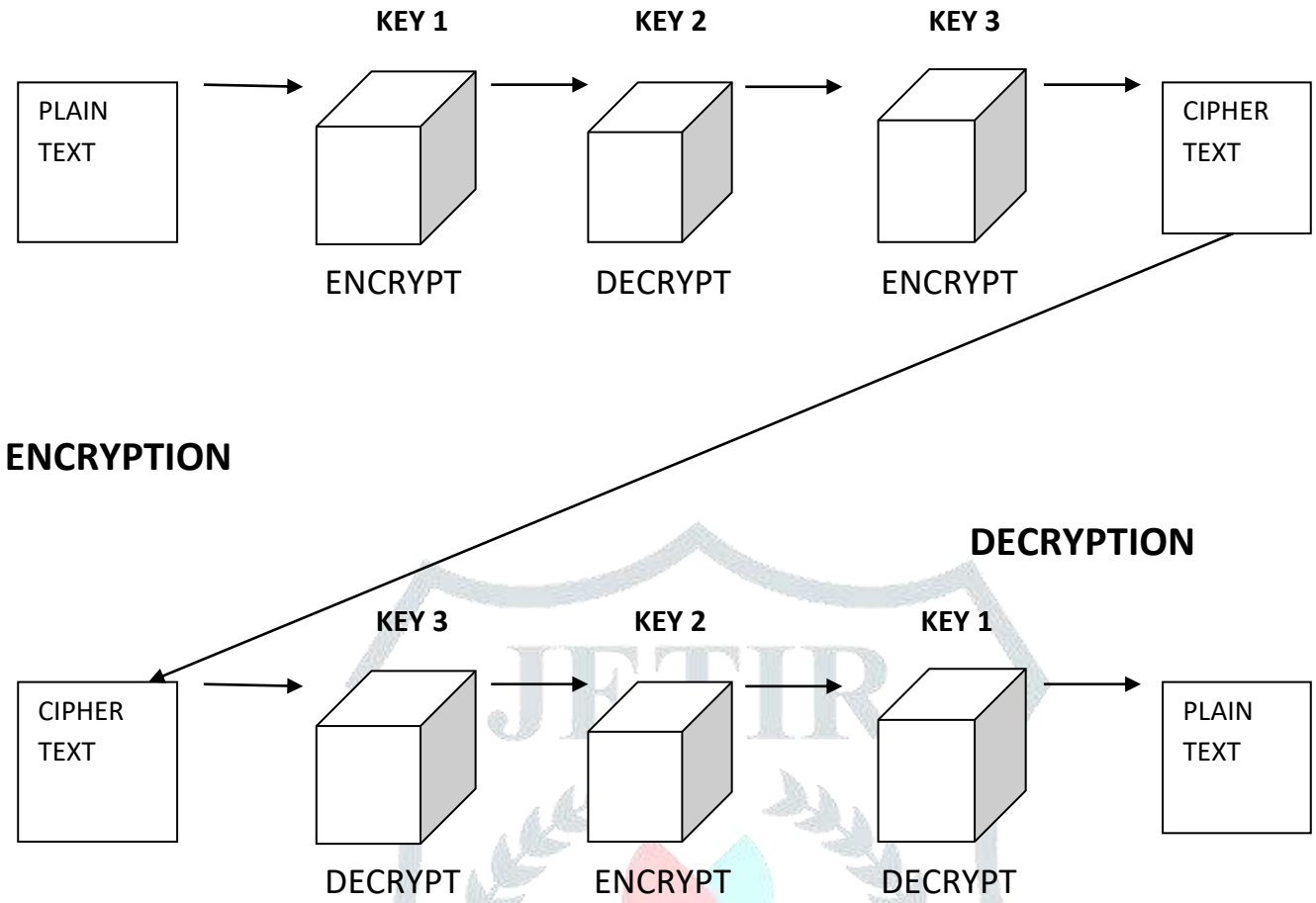
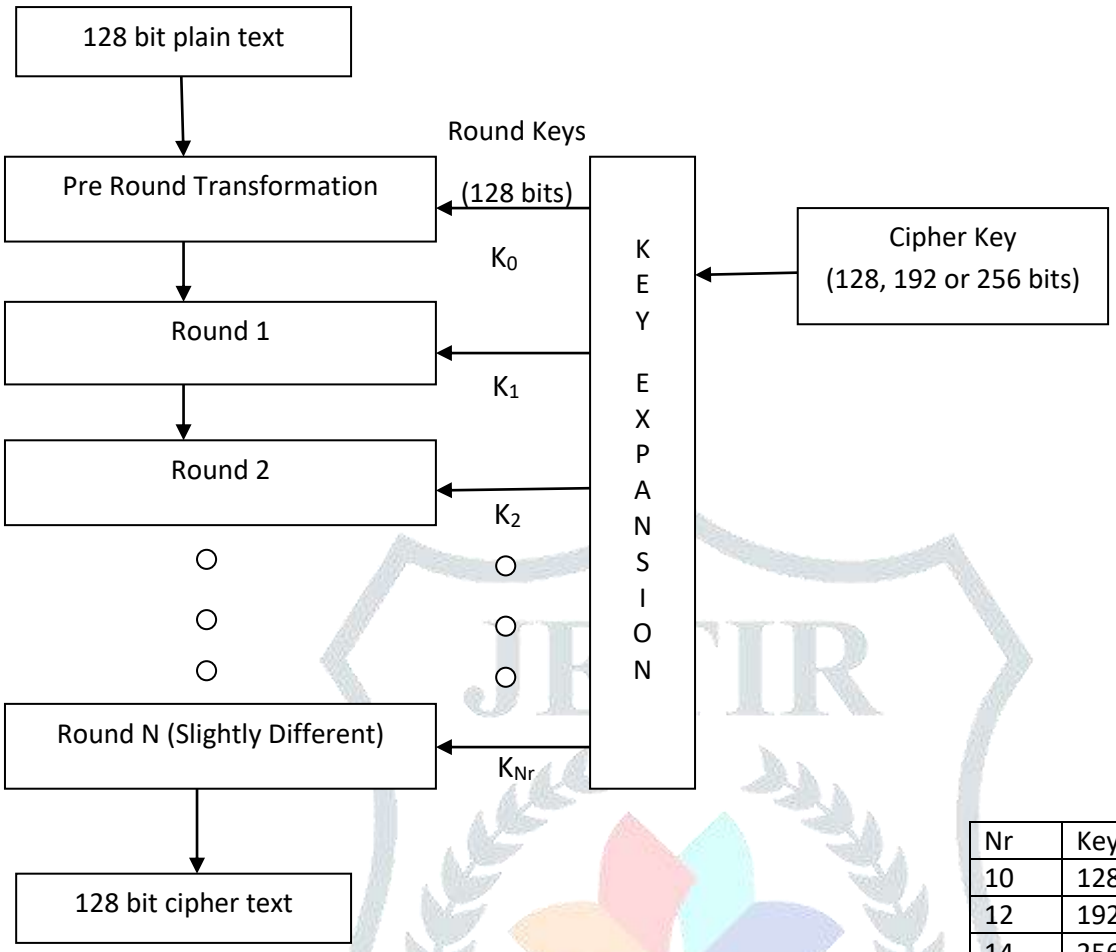


Fig: Symmetric Key(Triple DES Algorithm)

AES(Advanced encryption standard):AES is a symmetric key algorithm in which a single key is used for both encryption as well as decryption. In AES block size of 128 bits is fixed, and key lengths are varied which can be of 128-bits, 192-bits or 256-bits Depending on which version is used, the name of the standard is modified to AES-128, AES-192 or AES-256 respectively. AES differs from DES in that it is not a Feistel structure. A number of AES parameters depend on the key length. For example, if the key size used is 128 then the number of rounds is 10 whereas it is 12 and 14 for 192 and 256 bits respectively. At present the most common key size likely to be used is the 128 bit key.

RSA Algorithm: RSA algorithm has been named after Ron Rivest, Adi Shamir and Leonard Adleman.RSA is an asymmetric key algorithm. It uses different keys for encryption and decryption. It is based on a property of positive integers. RSA is an algorithm for public-key cryptography, involves a public key and a private key. The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted using the private key.
RSA uses two exponents, e and d, where e is public and d is private. Let the plaintext is M and C is cipher text, then at encryption $C = M^e \bmod n$ And at decryption side $M = C^d \bmod n$. Where n is a very large number, created during key generation process[2].
The field of information security has become a dynamic research area as the number of cyber attacks are increasing day by day. The conventional methods of encryption can only maintain the data security. The secret data can also be accessed by the unauthorised users for malicious purpose. Therefore it is essential to apply effective encryption/ decryption methods to improve data security[4]. Multi level encryption can be seen as a better option as compared to single encryption. Multi level encryption involved the encryption of an already encrypted message one or more times by using same algorithm with same key or same algorithms with different keys or by using different algorithms[13]. The choice depends on the application used. Since the multi level encrypted cipher text requires multiple computations therefore the cryptanalysis involved is much difficult as it requires more time and efforts. This means the multi level encrypted cipher text is much secure.



Nr	Key Size
10	128
12	192
14	256

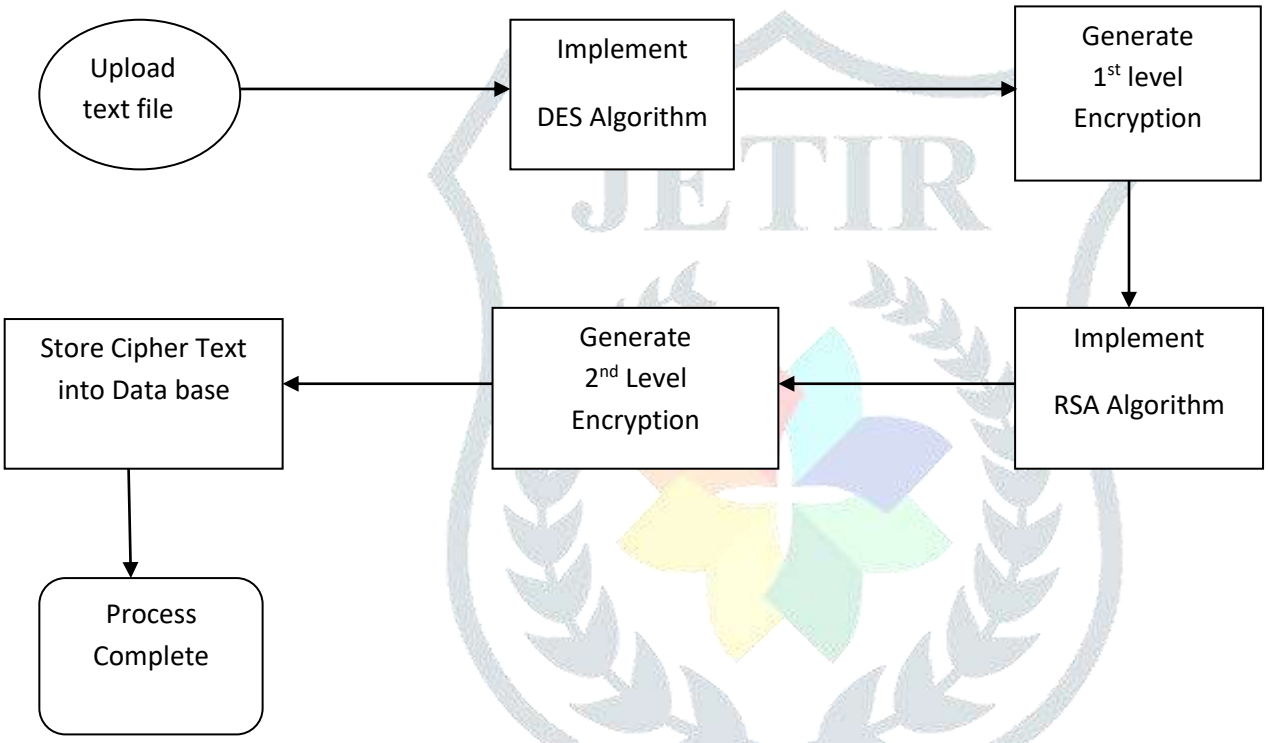
Fig. ENCRYPTION WITH AES

Examples to show conventional encryption and multi level encryption:

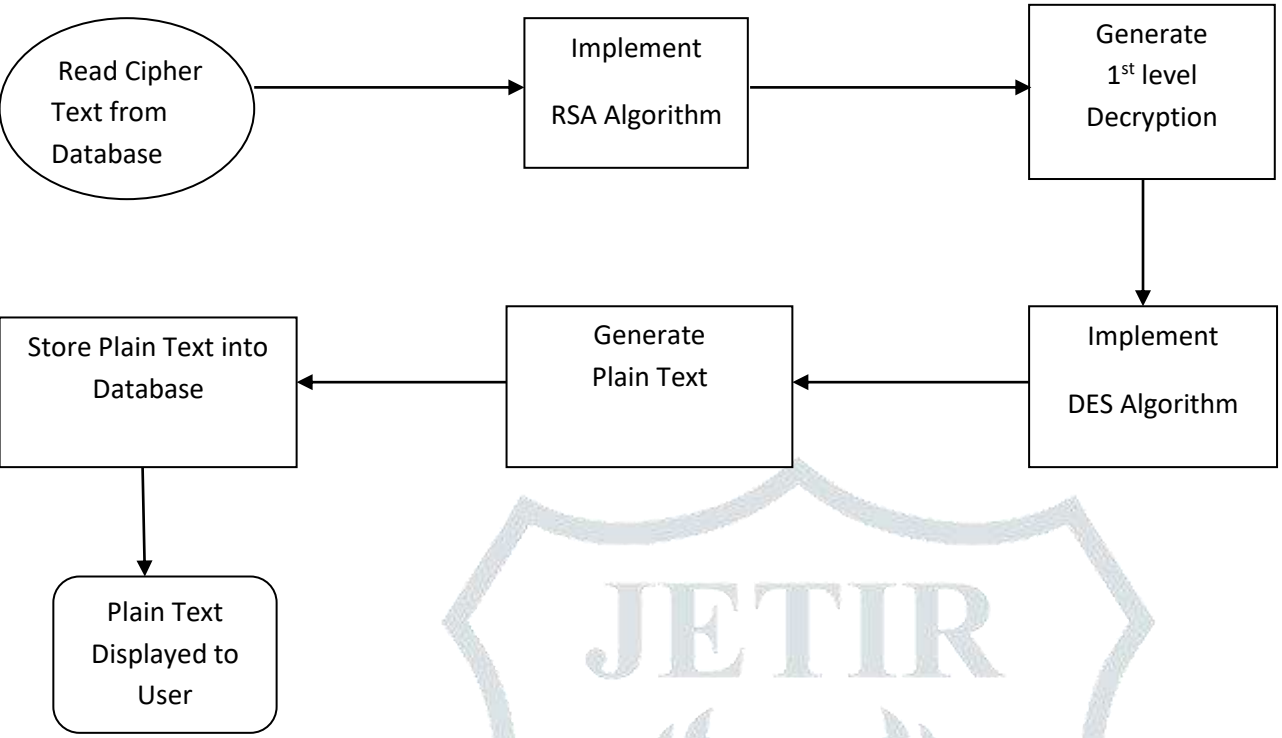
Plain text/original data : GALAXY
Algorithm(C): P+3
Cipher text : JDODAB
This is the conventional encryption.
If the message is encrypted twice with some block cipher, either with the same key or by using two different keys, the resultant encryption is expected to be stronger always except some cases. And by using three encryptions a greater level of security is expected.
Plain text/original data: GALAXY
Algorithm (C): ((P+3) +3) +.....3) (N times)
Cipher text: JDODAB (After first cycle)
MGRGDE (after second cycle)
PJUJGH (after third cycle)
.
.
.
Encrypted N times
In such a manner, multiple encryptions will occur in each phase and this process will be repeated number of times up to desired extent.
Multiple encryption when performed with different encryption keys is shown in next example
Plain text/original data: GALAXY
Algorithm (C): ((P+1)+3)+5.....N times)

Cipher text:
HBMBYZ (After first cycle)
KEPEBC (After second cycle)
PJUJGH (After third cycle)
Encrypted N times

As complexity increases in encryption algorithm, execution time may be increased but it enhances the data security enormously [13].
The multi level encryption algorithm for a cloud based data management system is shown. This algorithm is a combination of DES and RSA. In this system 1st level of encryption is generated by implementing DES algorithm. And then RSA algorithm is applied to the encrypted output of DES algorithm to generate 2nd level of encryption. Same process takes place for decryption using inverse DES and RSA algorithms [2].



BLOCK DIAGRAM OF MULTI LEVEL ENCRYPTION



BLOCK DIAGRAM OF MULTI LEVEL DECRYPTION

II. APPLICATIONS:

The main application fields of multi level encryption are

- SET(Secure Electronic Transactions)
- E commerce
- Secure voice communication
- Cloud security
- Secure access to XML documents
- VPN(Virtual Private Network)

III. LITERATURE SURVEY:

1. Surinder Kaur et al[1]observed and implemented parameters like time and for the implementation of multi level encryption used the Data Encryption standard(DES) and a modified version of RSA algorithm, the multi prime RSA.
2. Miss Shakeeba S. Khan et al[2] used multi level cryptographic algorithms to improve the security in cloud as per different perspectives of cloud customers.
3. Prof K.Govinda et al[3] provided multi level cryptographic technique for data encryption decryption using graceful codes.
4. Sunita Bhati et al[4] proposed a new encryption algorithm called as Byte rotation encryption algorithm (BREA)with parallel which improves the security as well as the speed of the encryption. This is an attempt to invent an encryption process which is very secure any very fast. The BREA is applied on different blocks of plaintext and executes in parallel manner through multithreading concept of single processor system.
5. Delson Therambath Rajanbabu et al[5] developed a Matlab based encryption tool which combinesvisual image encryption using template image fusion and symmetry cipher key cryptographic techniques The main aim was to construct a double verification check tool for the administrator identity before getting login access to the network..This provides a reliable and also a simple algorithm tool ensuring data privacy and integrity of the data stored inthe computers connected on the network.
6. Olawale S. Adebayo et al [6] implemented multilevel encryption algorithm using two cryptosystem; RSA and Substitution cryptosystem with one transformation per each. It presents an algorithmic paradigm which can be

implemented using any programming language. It simplifies the stages used for both encryption and decryption, presenting each stage in a sequential order.

7. Dr.Yasir Khalil Ibrahim et al[7] proposed "Multilevel Encryption Model" that adopts the basic principles of cryptography. It uses five symmetric keys (multiple) in floating point numbers, plaintext, substitution techniques and key combinations with unintelligible sequence to produce the ciphertext. The decryption process is also designed to reproduce the plaintext.
8. Thomas Hardjono et al[8] proposed an encryption scheme which allows a hierarchical organization of keys used to encrypt and decrypt data stored in databases. The scheme uses the same method as the RSA cryptosystem [RISH78] to encrypt and decrypt data, with additional restrictions on the availability of the encryption information to the public. Its security is based on the Discrete Logarithm problem [DIHE76] which is known to be NPI. Each user is issued a key which is used for decryption and user clearance verification.
9. Chandra Sekhara et al[9] focused on developing a multi encryption scheme with theexisting concepts like basis of a vectors spaces and linear transformations.
10. Dr Asoke Nath et al[10] introduced a symmetric, multilevel encryption algorithm which employs the use of feedback mechanism. It is a completely a new idea which may be implemented to send any kind of confidential data over internet. The detailed operation is controlled by the algorithm and in each instance by a key. This key is a secret parameter; ideally known only to the communicants for a specific message exchange context. The objective of this method is to evaluate the security of any confidential data. By using this algorithm one can encrypt any file such as .txt file, .doc file, .jpg file, .exe file, .wav file, .pdf file or with any other extension. After encryption or decryption, the original size of file will remain unaltered. A thorough investigation made on change in single bit in any position of the cipher text and it was found that decryption will not work. It is not possible to get back original plain text file if there is one change in bits in encrypted text. The testing is done on almost all types of files and it was found that the method is working satisfactorily.
11. Vinod Kumar Sharma et al[11] proposed the needs of multiple encryption technique in Secure Electronic Transaction to enhance the security of confidential data. This technique increases the data security in such a manner that unauthorized user can not access any part of information over wireless network as internet.
12. K.Satyanarayana[12]proposed an algorithm called Multilevel algorithm by using which an unauthorized user cannot access or modify the data or calculations of cloud. The work plan is to eliminate the concerns regarding data privacy using cryptographic algorithms to enhance the security in cloud as per different perspective of cloud customers.
13. Himanshu Gupta et al[13] proposed multi phase encryption technique where original data is encrypted many times with different strong encryption algorithms at each phase. This encryption technique enhancesthe complexity in encryption algorithm at large extent.
14. Mukesh Kumar Jha et al[14] proposedMulti LevelEncryption approach(MESCD)to protect data and resources on a cloud . In this work file is uploaded and encrypted using Nlevel of different keys.Further keys are merged into an single key 'K' which is again secure. Decryption processesis reverse of encryption where key (K) is spited into keys 'N' which is applied to decryption algorithm. Theproposed algorithm is effective and efficient then previously used HDFS approach.
15. Shweta Dahiya [15]Designed an effective and more secure image steganography algorithm using multi-level encryption. It is an improved report of existing single level encryption algorithm. Here the focus of concern is image because it is widely used in internet and also in mobile system. Enhanced Linear Significant Bit (LSB) algorithm can easily be executed and do not corrupt the image to the point of being noticeable. It would appear that improved LSB using Hadamard multi-level transform is more suitable algorithm of steganography due to its security. Using improved LSB algorithm secret messages can be exchanged over public channel in a safe way. The proposed method is more secure than the previously used method which uses only simple encryption because it is totally relied on the number of 1's in the equivalent binary value of the key.
16. M.Indhumathi et al [16] proposed multilevel algorithms to ensure that data security . By using multilevel encryption may provide more security for Cloud Storage than using only public key encryption

IV. CONCLUSION

Multi level Encryption is an ambivalent technique for data & information security and plays an important role in modern Cryptography. Multi level encryption describes the enhanced security as well as integrity of confidential data due to multiple encryption operations. The main advantage of multi level encryption is that it provides better security because even if some secret or encryption keys are cracked or some part of cipher texts are broken, the confidentiality and privacy of original data can still be maintained by multiple encryption. The multi level encryption enhances the data security enormously.

V. REFERENCES

[1] Surinder Kaur, Pooja Bharadwaj, Shivani Mankotia, "Study of Multi-Level Cryptography Algorithm: Multi-Prime RSA and DES", IJCNIS, Vol 09, 2017.

[2] Miss Shakeeba S. Khan, Prof. Ms. R. R. Tuteja, "Cloud Security Using Multilevel Encryption Algorithms", IJARCCE,Vol 05, No 01, 2016.

[3] Prof K.Govinda, Dr.E.Sathiyamoorth, "Multilevel cryptography technique using graceful codes", JGRCS, Vol 02, No 07, 2011.
[4] Sunita Bhati, Anita Bhati, S. K. Sharma, "A New Approach towards Encryption Schemes:Byte – Rotation Encryption Algorithm", WCECS, Vol II, 2012.
[5] Delson Therambath Rajanbabu, Chaithanya Raj, "Multi Level Encryption and Decryption Tool for Secure Administrator Login over the Network", INDJST, Vol 07(S4), 2014.
[6] Olawale S. Adebayo, Morufu Olalere, Joel N. Ugwu, " Implementation of N-Cryptographic Multilevel Cryptography Using RSA and Substitution Cryptosystem", MIS Review, Vol 20, No 02, 2015.
[7] Dr.Yasir Khalil Ibrahim,"New Technique Using Multiple Symmetric keys for Multilevel Encryption", Vol 06, Issue 03, 2016.
[8] Thomas Hardjono, Jennifer Seberry, "Proceedings of ACSC-12, University of Wollongong", 1989.
[9] A. Chandra Sekhar, V. Anusha, B. Ravi Kumar & S. Ashok Kumar, "Journal of Information and OptimizationSciences", Vol 36, No 04, 2015.
[10] Dr Asoke Nath, Soumyadip Basu, Aritra Chandra, Noor ur Rahman, " Tsunami Encryption Algorithm", IJARCSMS, Vol 05, 2017.
[11] Himanshu Gupta, Vinod Kumar Sharma, "Role Of Multiple Encryption In Secure Electronic Transaction", IJNSA, Vol 03, No 06, 2011.
[12] K.Satyanarayana, "Multilevel Security for Cloud Storage using Encryption Algorithms", IJECS, Vol 05, 2016.
[13] Himanshu Gupta, Vinod Kumar Sharma, "Multiphase Encryption: A New Concept in Modern Cryptography", IJCTE, Vol 05, No 4, 2013.
[14] Mukesh Kumar Jha, Veerendra Shrivastava, "Multi Level Encryption Approach To Secure Cloud Data", IJESRT, Vol 05, 2016.
[15] Shweta Dahiya, " Multilevel Data Encryption Using Hadamard Transform Based Image Steganography",IJEDR, Vol 04, 2016.
[16] M.Indhumathi,B.Salai Nalvetham, R.Venkatesh, "Multilevel Security On Cloud Computing With Cryptography Algorithm", IJMTER, Vol. 03, 2016.