IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 1, Ver. III (Jan – Feb. 2015), PP 62-69
www.iosrjournals.org

Comparison of Various Encryption Algorithms and Techniques for improving secured data Communication

[1]Soheila Omer AL Faroog Mohammed Koko, [2]Dr.Amin Babiker A/Nabi Mustafa
[1] AL Neelain University, Faculty of Engineering . Khartoum,Sudan
[2] Dean of Faculty of Engineerning , AL Neelain University, Khartoum, Sudan

Abstract: *Information security is the process of protecting information. It protects its availability, privacy and integrity. Access to stored information on computer databases has increased greatly. More companies store business and individual information on computer than ever before. Much of the information stored is highly confidential and not for public viewing.*

To write this paper we have Study about information security using cryptography technique. After the detailed study of Network security using cryptography, I am presenting my proposed work. This paper is dividing in four sections contain of basic introduction about Information Security using cryptography, detailed description of Information security using cryptography and various algorithms, also; we are presenting proposed algorithm, Presenting summary and references where we have completed my research. The proposed algorithm has the batter speed compared with the comparing encryption algorithm. Nevertheless, the proposed algorithm improves encryption security by inserting the symmetric layer. The proposed algorithm will be useful to the applications which require the same procedure of encryption and decryption.

In this paper also, we have developed a new cryptography algorithm which is based on block cipher concept. In this algorithm we have used logical operation like XOR and shifting operation. Experimental results show that proposed algorithm are very efficient and secured, and this paper covers the various techniques and algorithms used for the data security.

Keywords: *Information security, Encryption, Decryption, Cryptography*

I. Introduction

Data security is an essential part of an organization; it can be achieved by the using various methods. That to maintain and upgrade the model still efforts are required and increase the marginally overheads. The encrypted data is safe for some time but never think it is permanently safe. After the time goes on there is chance of hacking the data by the hacker. Fake files are transmitted in the same manner as one can sends the encrypted data. The information about the key is present in the encrypt data which solves the problem of secure transport of keys from the transmitter to receiver . In case of practical system encrypted data is passed through the various stations which are capable to re-encrypt the data by their own key. At the time the previous keys are discarded, this will make the system more secure. There are many algorithms available in the market for encrypting the data. Encryption is the process in which plaintext has been converted into the encoded format cipher text with the help of key.

II. Methodology

In this paper, we have considered Various Encryption Algorithms and Techniques for improving secured data Communication, Information Security using cryptography, detailed description of Information security using cryptography and various algorithms; also, we have developed a new cryptography algorithm which is based on block cipher concept, like XOR and shifting operation.

III. Results

- **Summary of algorithms**

We compare measured speed of encryption with various algorithms available as standard in Sun's JDK, and then give a summary of various other characteristics of those algorithms. The encryption algorithms is consider here are AES (with 128 and 256-bit keys), DES, Triple DES, RC4 (with a 256-bit key) and Blowfish (with a 256-bit key).

Performance

First, the easy bit. Figure 1 shows the time taken to encrypt various numbers of 16-byte blocks of data using the algorithms mentioned.

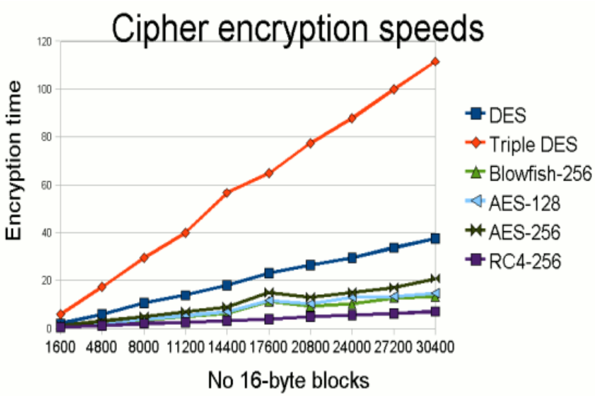

Fig4 Comparison of encryption times for various common symmetric encryption algorithms

It's important to note right from the beginning that beyond some ridiculous point, it's not worth sacrificing speed for security. However, the measurements will still help us make certain decisions.

Characteristics

Table 1: gives a summary of the main features of each encryption algorithm, with what I believe is a fair overview of the algorithm's current security status.

Table 1: Characteristics of commonly used encryption algorithms

Algorithm	RC4	Blowfish	AES	DES	Triple DES
Key size(s)	40-1024	128-448	128, 192, 256	56	112/168, but equivalent security of 80/112
Speed	Very fast	Fast	Fast	Slow	Very slow
Speed depends on key size	No	No	Yes	Yes	No
Security / comments	Of questionable security; may be secure for moderate numbers of encrypted sessions of moderate length. RC4 has the redeeming feature of being fast. However, it has various weaknesses in the random number sequence that it uses: see Klein (2008)1.	Believed secure, but with less attempted cryptanalysis than other algorithms. Attempts to cryptanalyse Blowfish soon after publication are promising (Schneier, 19952 & 19963). But, unlike AES, it doesn't appear to have received much attention recently in the cryptographic literature. Blowfish has been superseded by Twofish, but the latter is not supported as standard in Java (at least, not in Sun's JDK).	Secure, though with some reservations from the crypto community. It has the advantage of allowing a 256-bit key size, which should protect against certain future attacks (collision attacks and potential quantum computing algorithms) that would have 264 complexity with a 128-bit key and could become viable in the lifetime of your data	Insecure: A $10,000 Copacobana machine can find a DES key in an average of a week, as (probably) could a botnet with thousands of machines.The simple answer is: "Don't use it– it's not safe". (RFC 4772).	Insecure: A $10,000 Copacobana machine can find a DES key in an average of a week, as (probably) could a botnet with thousands of machines.The simple answer is: "Don't use it– it's not safe". (RFC 4772).

IV. Discussion

4.1 Cryptography

Cryptography, it's the idea of storing and transmitting data in a form that only the authorized parties can interpret. The conversion of data into a secret code for transmission over a public network. Today, most cryptography is digital, and the original text ("plaintext") is turned into a coded equivalent called "cipher text" via an encryption algorithm. The cipher text is decrypted at the receiving end and turned back into plaintext and for secured data communications It is a technique used to avoid unauthorized access of data. The encryption process consists of single or multiple keys to hide the data from the intruders. The original text before the encryption process is known as Plaintext.The text obtain after encoding the data with the help of a key is known as cipher text. For the encryption Process has the power to change/upgrade the key at any time and information of changed or upgraded key has been made known to both the parties. The encryption, decryption, and key are shown in the figure 1.

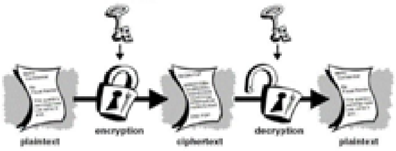

Figure 1: block diagram of cryptographic model

4.2 Types Of Cryptography

The cryptography techniques are classified on the basis of their key selection. The section shows the merits and merits of various cryptographic techniques.

4.2.1 Symmetric (Private) Cryptography

Symmetric (also called private-key encryption or secret-key encryption) involves using the same key for encryption and decryption.

Encryption involves applying an operation (an algorithm) to the data to be encrypted using the private key to make them unintelligible. The slightest algorithm (such as an exclusive OR) can make the system nearly tamper proof (there being so such thing as absolute security).

users have the provision to update the keys and use them to derive the sub keys. It is much effective and fast approach as compared to asymmetrical key cryptography. In symmetrical key cryptography; key has been generated by the encryption algorithm and then send it to the receiver section and decryption takes place.

4.2.2 Asymmetric (Public) Cryptography

Asymmetric cryptography is cryptography in which a pair of keys is used to encrypt and decrypt a message so that it arrives securely. Initially, a network user requests a public and private key pair. A user who wants to send an encrypted message can get the intended recipient's public key from a public administrator . The method is more secured as compared to private key cryptography but it consumes more power and takes more processing time therefore extra hardware is required. Due to increase in the computational unit the overheads are high in public key cryptography.

4.3 Modern Cryptography

A combination of both public key and private key cryptography is known as modern cryptography. A pair of public and private keys has been used to encrypt and decrypt the data. The technique has the salient features of private key; fast speed, easy to process and features of public key such as secured, avoid key transportation, provide the power to the users to generate their own keys of variable length. Users also have the flexibility to upgrade the key at any interval of time. In this technique; certification authority has been used to keep the track of the entire system and keys.

4.4 Cryptographic Algorithm

The generation, modification and transportation of keys have been done by the encryption algorithm. It is also named as cryptographic algorithm. There are many cryptographic algorithms available in the market to encrypt the data. Their strengths depend upon the cryptographic system. Any computer system which involves cryptography is known as cryptographic system, the strength of encryption algorithm heavily relay on the computer system used for the generation of keys. The computer systems take the responsibilities sending the secret information over the web with the help of cryptographic hash functions, key management and digital signatures. Crypto systems are composed from cryptographic primitives such as encryption algorithm, number of keys, hash and round functions, memory elements, real time operating system, etc.

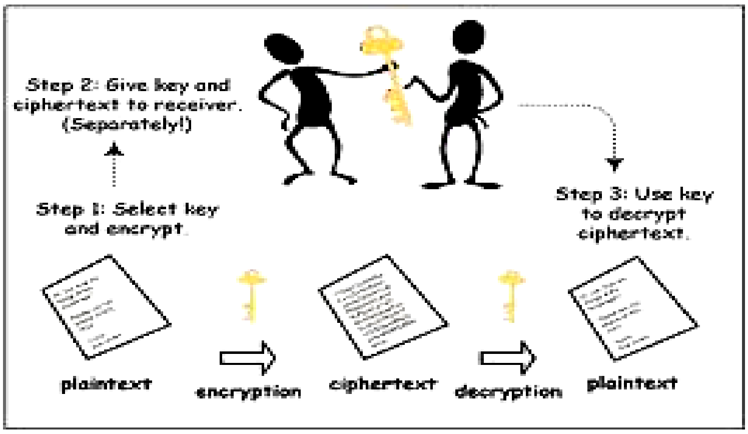
Step 2: Give key and ciphertext to receiver. (Separately!)
Step 1: Select key and encrypt.
Step 3: Use key to decrypt ciphertext.
plaintext
encryption
ciphertext
decryption
plaintext

Fig 2: Diagram show Cryptographic Algorithm

4.5 Some important encryption algorithms are discussed here:

4.5.1 Data Encryption Standard (DES)

It is one of the most widely accepted, publicly available cryptographic systems today. It was developed by IBM in the 1970s but was later adopted by the US government as a national bureau of standards as an official Federal Information Processing Standard (FIPS) for the United States in 1976. It uses a 56-bit key to encrypt the 64 bit block size data. It processes 64-bit inputs into 64-bit cipher-text and algorithm performs 16 iterations.

4.5.2 International Data Encryption Algorithm (IDEA)

IDEA is a block cipher designed by James Massey and Xuejia Lai and was first described in 1991. It uses 128 bit key length which operates on 64 bit blocks. It consists of a series of eight identical transformations based upon bitwise exclusive-or, addition and multiplication modules. It is based upon symmetric cipher and has very weak key design method therefore security level of the algorithm is very poor as compared to the DES. IDEA not becomes so much popular due to its complex structure.

4.5.3 Blowfish

Blowfish is a symmetric-key block cipher, designed in 1993 by Bruce Schneier and included in a large number of cipher suites and encryption products. Blowfish provides a good encryption rate in software and no effective cryptanalysis of it has been found to date. However, the Advanced Encryption Standard (AES) now receives more attention.

Schneier designed Blowfish as a general-purpose algorithm, intended as an alternative to the aging DES and free of the problems and constraints associated with other algorithms. At the time Blowfish was released, many other designs were proprietary, encumbered by patents or were commercial or government secrets. Schneier has stated that, "Blowfish is unpatented, and will remain so in all countries. The algorithm is hereby placed in the public, and can be freely used by anyone."
Notable features of the design include key-dependent S-boxes and a highly complex key schedule.

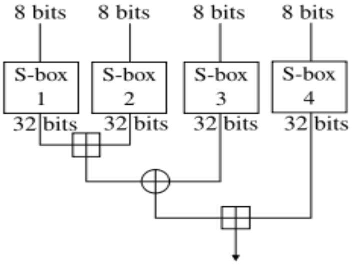

Fig 3: Blowfish Cryptographic Algorithm

4.5.4 Triple DES (TDES)

It was developed in 1998 and derived from DES. It applies the DES cipher algorithm three times to each of the data blocks. Triple Data Encryption Standard (DES) is a type of computerized cryptography where block cipher algorithms are applied three times to each data block. The key size is increased in Triple DES to ensure additional security through encryption capabilities. Each block contains 64 bits of data. Three keys are referred to as bundle keys with 56 bits per key. There are three keying options in data encryption standards:
All keys being independent Key 1 and key 2 being independent keys All three keys being identical

Key option #3 is known as triple DES. The triple DES key length contains 168 bits but the key security falls to 112 bits.

4.5.5 Advanced Encryption Standard (AES)

It is a symmetric 128-bitblock data encryption technique developed by Belgian cryptographers Joan Daemen and Vincent Rijmen. The U.S government adopted the algorithm as its encryption technique in October 2000, replacing the DES encryption it used. AES works at multiple network layers simultaneously. The National Institute of Standards and Technology (NIST) of the U.S. Department of Commerce selected the algorithm, called Rijndael (pronounced Rhine Dahl or Rain Doll), out of a group of five algorithms under consideration, including one called MARS from a large research team at IBM.

While the terms AES and Rijndael are used interchangeably, there are some differences between the two. AES has a fixed block size of 128-bits and a key size of 128, 192, or 256-bits, whereas Rijndael can be specified with any key and block sizes in a multiple of 32-bits, with a minimum of 128-bits and a maximum of 256-bits.

4.5.6 Twofish

It was derived from blowfish by Bruce Schneier in 1998. It is freely available in the public domain as it has not been patented. It is a symmetric key block cipher having key sizes 128,192 and 256 bits used to encrypt the 128 bit block size data in 16 rounds. The algorithm making use of S- Boxes and makes the key generation process very complex and secured.

4.5.7 RSA

RSA is a public key system designed by Ron Rivest, Adi Shamir, and Leonard Adleman in 1978. The RSA operations can be decomposed in three broad steps; key generation, encryption and decryption. Two distinct prime number say p&q has been selected randomly and then

by using the mathematical properties such as Euler's function, Chinese remainder theorem, hamming weight and exponential functions key has been generated and then encryption process takes place. Decryption has been done in the receiver section by using the public key concept.

RSA have many flaws in its design therefore not preferred for the commercial use. When the small values of p&q are selected for the designing of key then the encryption process becomes too weak and one can be able to decrypt the data by using random probability theory and side channel attacks. On the other hand if large p&q lengths are selected then it consumes more time and the performance gets degraded in comparison with DES.

Further, the algorithm also requires of similar lengths for p&q, practically this is very tough conditions to satisfy. Padding techniques are required in such cases increases the systems overheads by taking more processing time.

4.5.8 Diffie-Hellman

Whitfield Diffie and Martin Hellman introduce the key exchange technique in 1976. In 2002, Ralph Merkle's contributed his work in the key exchange program and the technique named as Diffie Hellman Merkle key exchange.

In order to tackle man in the middle attacks the Diffie Hellman introduces password authenticated key agreement (PAKE) which was based on generating matrix.

When hacker uses single password attack in the iteration; immediately the key structure becomes changed, thus allows only maximum of single password attack in the each iteration by the hacker. This technique helps in achieving better security even in the presence of weak password.

4.5.9 Elliptic Curve Cryptography (ECC)

In 1985, Neal Koblitz and Victor S. Miller suggested the use of ECC for the encryption of data. There are four ECC techniques and stated as: the elliptic curve Diffie Hellman key agreement scheme which uses the key exchange approach suggested by Diffie Hellman scheme and based

Upon the public key cryptography. Second, the Elliptic Curve Integrated Encryption Scheme (ECIES) in which encryption and key generation takes place in one step.

Third scheme was based upon the digital signature algorithm and is known as Elliptic Curve Digital Signature Algorithm. MQV key agreement scheme has been used in the ECMQV. The security pattern of ECC is quite remarkable and does not affect by the side channel attacks

Variable key lengths have been used for the encryption and are varied in accordance with the data blocks to provide sufficient amount of cover the data.

4.5.10 Pretty Good Privacy (PGP)

In 1991 the Philip Zimmermann developed Pretty Good Privacy (PGP) public key cryptography programs. The algorithm was supported by Linux and Window operating systems. It combines the private and public key cryptography to maintain the appropriate confidential level. The technique can be used to encrypt the e-mail messages with the help of hash and MD5.

4.5.11 Public key infrastructure (PKI)

It is an unsymmetrical cryptography technique used to encrypt the e- mails. The public keys of the users are covered up with the certificates created by trusted third party. From the root level different keys were designed for different users and are always kept unknown from each other. The first key was generated by the algorithm for the encryption and always kept secret; the second key was generated by the CA on the request of the users and publicly circulated. The user can update their keys and the duplicate copy of the new key was stored at CA.

V. Aesaes

Stands for Advanced Encryption Standard and is actually an algorithm that was originally called Rijndael, after its anything else:

- it is a politically safe decision: the encryption standard of the US National Institute of Standards and Technology (NIST), and the US government reportedly approves AES with 192 or 256-bit keys for encrypting top secret documents (or put
- another way, your boss won't sack you for choosing AES...);
- it is largely considered secure, though with some reservations:
- nobody yet has (publicly) a full attack on AES, or a partial attack that is practical (though some impractical partial attacks exist5);
- however, AES is algebraically simpler than other block ciphers: effectively, it can be written as a series of mathematical equations, and there is a worry that somebody could demonstrate a way to solve those equations (see Ferguson & Schneier, Practical Cryptography, pp. 57-58);
- the NSA may have chosen Rijndael as they secretly know how to break it, or secretly estimated that they could develop a way to break it.
- It is fast (Ferguson & Schneier (op cit), p. 59, argue that this is the reason it was picked over Serpent as the AES standard).

VI. Criteria of a cryptographic algorithm

The security of the model has been analysis on the basis of their encryption algorithm and the key management. It has been observed that the encryption algorithm have their own characteristics; one algorithm provides security at the cost of hardware, other is reliable but uses more number of keys, one takes more processing time. This section shows the various parameters which plays an important role while selecting the cryptographic algorithm.

6.1 Level of Protection

The techniques have been compared on the basis of that how much:

- CPU time would be required by a machine for a given processing speed to generate the key, encrypt and decrypt the data.
- The amount of memory required to hold the data in encryption process.
- Number of users accommodated by the model.
- Time required by the model to recover the data in case of key failure.
- Time available to the hacker to produce various types of attacks.

6.2 Complexity

Key generation and encryption techniques are usually based upon the mathematical properties of numbers and functions. Higher order polynomial cause complex system as a result the probability of error is increased. If the keys are based upon orthogonal principle then same key must be selected at the receiver to recover the data. Let us take a case in which A is the data stream which has been encrypted by the key B. At the receiver side same key has used to decrypt the data; if key has been changed from B to ' B then one cannot recover the data as shown in case-2.

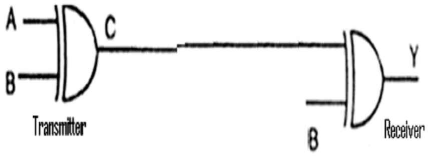

Figure 5. Encryption and decryption by using same key

Case-1: Using same key B for encryption and decryption

$$C = A\overline{B} + B\overline{A}$$
$$Y = C \oplus B$$
$$Y = \left(\left(A\overline{B} + B\overline{A}\right)\right) \oplus B$$
$$Y = A$$

Case-2: Using different key for encryption B and decryption

$$C = A\overline{B} + B\overline{A}$$
$$Y = C \oplus B'$$
$$Y = \left(\left(A\overline{B} + B\overline{A}\right)\right) \oplus B'$$
$$Y = \left(A\overline{B} + B\overline{A}\right)\overline{B'} + \overline{\left(A\overline{B} + B\overline{A}\right)}B'$$

This is not equal to the original data, Y ≠A

The selection of algorithm also depends upon the requirement of security level. If short data sequences are present within the organization and moderate security level is required then one can make use of symmetrical key cryptography, On the other hand if average security level is needed over the web then pretty good privacy maybe selected. For highly secured model one can make use of DES or AES having more number of round functions. The known numbers of attacks up to 2006 are given as: 7 rounds for 128-bit keys, 8 rounds for 192-bit keys, and 9 rounds for 256-bit keys therefore DES and AES can be used to sufficient amount of security level.

6.4 Available Algorithms

Few encryption algorithms are patented and are not freely publicly available. Moreover, there are some legal liabilities are also associated with these encryption algorithms. While selecting an encryption algorithm it has been taken care that which algorithm is suitable and publicly available for the encryption purpose.

6.5 Overheads

Cryptography requires continuous efforts to achieve security; initially efforts are required in the generation of keys. Once the keys have been generated the next step is to encrypt the data and send it over the web. There are various overheads which are associated with in the cryptography and are given as:

- Financial overheads: a lot of money has been invested to keep the documents secured from the enemy.
- Less Channel bandwidth: the users have been able to utilize only limited bandwidth due the presence of additional bits caused by keys.
- More Heat Dissipation: While encrypting the data with multiple keys having large lengths results in significant amount of heat dissipation has been observed. This will put up a limitation on the use of On-chip components which are highly desirable for the fast encryption process.
- Power consumption: the powerful processors consume more power in the key generation process as a result node capacitance, charge sharing and leakage current exist in the model. These parameters are responsible for the loss of data and cause station failure.
- Delay: the encryption process takes time to convert the plain text into cipher text which causes delay and increases latency. Few encryption algorithms also require additional padding techniques which also consumes more power and time.

6.6 Key management

In modern key cryptography every user wants to send or receive secured electronic mail. Users have their own keys and it is required to keep their keys and information about their data must be kept secret from each other. In practice, the keys used by the individual user are different from each other. But in a networked environment, the user might need to use an e-mail from multiple computers having different operating systems. The padding techniques are also the main cause of delay which results in timing collisions in dynamic multiuser system. It creates the need of key sharing scheme. Number of keys, length of keys and their generation and transportation are concerned with security level of data. The aim is to make the entire model secured; all the nodes should be monitored continuously in order to make the combination secured. During the attacks there are few possible outcomes, hacker can be

- Able to break the other node,
- attacks the other nodes but does not get succeeded; at this time the attacked node get failed due to the efforts done by the hacker,
- Attacks the node and succeeded to break it but not able to access the data (due to presence of second key), in such case the hacker corrupts the data as a result the accuracy and reliability of data decreases.

The best method to encounter the problem is that to use multiple keys for individual nodes. When the failure rate of the first key is increased then use the second key for the re-encryption the data. At the same time generate the new key as a replacement of the first key. The probability of failure of both key is very less, in rare cases it exits and such cases are handled; either by employing more number of keys or data sequences is divided into small sequences. In such cases the short length data sequences are used in order to provide sufficient time to the algorithm to generate the new keys.

VII. Conclusion

The study of various techniques and algorithms used for the secured communication in MN has been done. From the related work it has been observed that the strength of model depends upon the key management, type of cryptography, number of keys, number of bits used in a key. Longer key length and data length consumes more power and results in more heat dissipation. So, it is not advisable to use short data sequence and key lengths because by using powerful software's one can hack the short keys very easily and able to break the system. Once one can determine the failure rate of keys then encryption process takes place. All the keys are based upon the mathematical properties and their strength decreases. So, basically it is a tradeoff between key length and security level. For the task the optimal selection of keys makes the model optimized. The keys having more number of bits requires more computation time which simply indicates that the system takes more time to encrypt the data.

References

[1]. Ajay Kakkar, Dr. M. L. Singh, Dr. P. K. Bansal, “Efficient Key Mechanisms in Multinode Network for Secured Data Transmission”, International Journal of 92 Engineering Science and Technology, Vol. 2, Issue 5, 2010, pp.787-795.

[2]. Davis, R, “The data encryption standard in perspective”, Communications Society Magazine, IEEE, 2003, pp. 5-9.

[3]. Ajay Kakkar, M. L. Singh, P.K. Bansal," Comparison of Various Encryption Algorithms and Techniques for Secured Data Communication in Multinode Network", International Journal of Engineering and Technology Volume 2 No. 1, January, 2012.

[4]. Diffiee, W., and Hellman, M., “New Directions in Cryptography”, IEEE Transaction Information Theory IT-22, (Nov. 1976), pp. 644-654.

[5]. Vishwa gupta, Gajendra Singh ,.Ravindra Gupta," Advance cryptography algorithm for improving data security", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 1, January 2012 ISSN: 2277 128X.

[6]. Suyash Verma, Rajnish Choubey,Roopali soni, "An Efficient Developed New Symmetric Key Cryptography Algorithm for Information Security", International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, Volume 2, Issue 7, July 2012) 18 .