A New Method for Symmetric Key Cryptography

B. Nagaraju
Research Scholar, Dept. of CSE University College of Engineering,
Osmania University, Hyderabad,India

P. Ramkumar, PhD
Professor, Department of CSE,
University College of Engineering,
Osmania University, Hyderabad,India.

ABSTRACT
In the age of Information Technology Information Security is very important. To provide the security to the communication data, we are using different encryption algorithms. Encryption algorithms can be categorized into Symmetric key cryptography and Asymmetric key cryptography. Many of the Symmetric encryption algorithms (DES, 3DES, Blowfish, RC6 etc…) following the feistel structure, some algorithms (AES etc...) are following substitutions, permutations structure. These all are block ciphers. Symmetric Encryption Algorithms encrypting the plain text by using the secret key and producing cipher text. Decryption algorithms takes the cipher text and secret key and produces the original plain text, this is basically the encryption algorithm run in reverse. This paper specifies a new method for Symmetric key cryptography that can be used to protect data which is transferred through internet. This algorithm is not following the feistel structure, substitutions and permutations. This algorithm can be used for stream ciphers and block ciphers.

Keywords
Symmetric key cryptography, Plain text, Cipher text, Secret key, Encryption algorithm Decryption algorithm, Rasilabdacheda misravibhaga sutram, Divisor, Dividend, Quotient.

1. INTRODUCTION
In this age of universal electronic connectivity, Information Security is an important issue. To provide the secure communication between the communication parties, we are using Cryptography concept. Cryptography means "secret writing" [4].It is the word with Greek origin. Cryptography is the scientific study of methods for securing digital message transactions and distributed computations [3]. Cryptography algorithms can be categorized into Symmetric Key Cryptography (Secret Key Cryptography or Conventional Encryption) and Asymmetric Key Cryptography (Public Key Cryptography). Conventional algorithms are further divided into two types. Those are stream ciphers and block ciphers.

Conventional Encryption method performs the encryption and decryption using a single secret key. The single secret key must be shared between the both sender and receiver in secure manner. It is also known as symmetric key cryptography or secret key cryptography. Secret key encryption method converts the plain text into cipher text using the shared secret key and an encryption algorithm. Using the same shared secret key and a decryption algorithm, cipher text is converted into plain text [5].

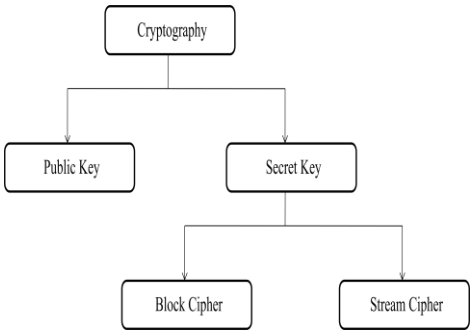


Fig 1: Classification of Cryptography

Conventional Encryption method performs the encryption and decryption using a single secret key. The single secret key must be shared between the both sender and receiver in secure manner. It is also known as symmetric key cryptography or secret key cryptography. Secret key encryption method converts the plain text into cipher text using the shared secret key and an encryption algorithm. Using the same shared secret key and a decryption algorithm, cipher text is converted into plain text [5].

Public key encryption method performs the encryption and decryption using the two different keys-one is called as public key and another one is called as private key. This method is also known as asymmetric key cryptography. Public key encryption method converts the plain text into cipher text using a one key from the existing two keys and an encryption algorithm. Using the matched key and a decryption algorithm, cipher text is converted into the original plain text [5].

Conventional encryption algorithms are of two types: stream ciphers and block ciphers. Let P be a plaintext and let $p_1p_2.....p_m \in P$ be a plaintext string. Let K be a key and let $k_1k_2 \cdot \cdot \cdot k_n \in K$ be a key stream. This cryptosystem is called a stream cipher if encryption algorithm applied on plaintext stream $p_1p_2.....p_m$ is accomplished by repeated application of the encrypting transformation on plaintext message units, $Enc(p_j,k_j) = c_j$, and if d_j is the inverse of k_j, then decrypting takes place as $Dec(c_j,d_j) = p_j$ for $j \geq l$. If there exists an $l \in$ Q such that $k_{j+l} = k_j$ for all $j \in Q$, then the stream cipher is called as periodic with period l. A Block Cipher is a cryptosystem that breaks up the plaintext message into strings, called blocks, of fixed length $k \in Q$, called the block length and encrypts one block at a time [6].

2. SYMMETRIC CIPHER MODEL
A conventional encryption system has following key components (Figure. 2):

• *Plaintext:*
This is the original message or information that is send into the encryption algorithm as one of the inputs.

• *Encryption algorithm:*
The encryption algorithm takes plaintext and secret key as inputs. The algorithm executes several substitutions and transformations on the plaintext and gives cipher text as output.

• *Secret key:*
The secret key is one of inputs to the encryption and decryption algorithms. The key is a value independent of the plain text and of the algorithm. The algorithm will give a different output depending on the specific key being used at the time. The exact substitutions and transformations performed by the algorithm depend on the key.

• *Cipher text:*
This is the jumbled message produced as output from the encryption algorithm. It depends on the plaintext and the secret key. For a given data, two different keys will produce two different cipher texts. The cipher text is a random stream of data.

• *Decryption algorithm:*
This is essentially the encryption algorithm run in reverse. It takes the cipher text and the secret key as inputs and gives the original plaintext as output.

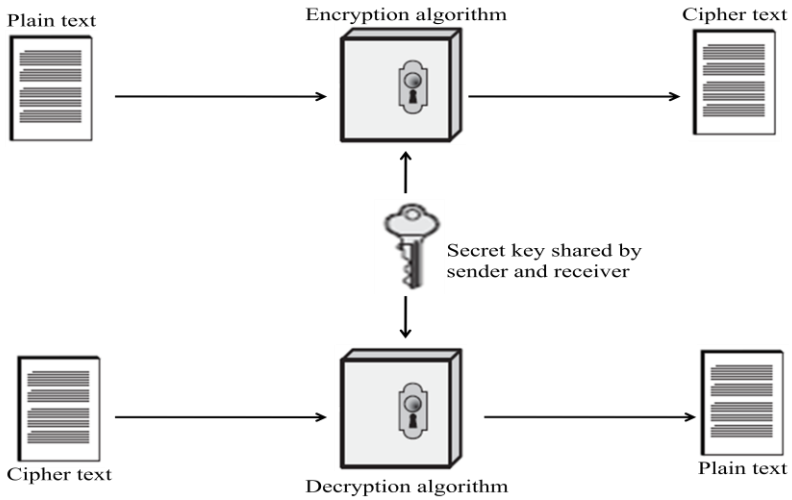


Fig.2: Simplified Model of Conventional Encryption

There are two necessities for secure use of conventional encryption:

1. The encryption algorithm should be strong. At a minimum, the algorithm to be such that an adversary who knows the algorithm and has access to one or more cipher texts would be unable to decrypt the cipher text or find out the key. This necessity is generally expressed in a stronger form: The adversary should be unable to decrypt cipher text or discover the key even if he or she is in possession of a number of cipher texts together with the plaintext that produced each cipher text.

2. Sender and receiver must have received copies of the secret key in a secure manner and must keep the key secure. If someone can discover the key and knows the encryption algorithm, all communication using this key is decipherable. We assume that it is impractical to decipher a message on the basis of the cipher text and knowledge of the encryption or decryption algorithm. In other words, the algorithm need not be secret; only the key should be secret. This feature of conventional encryption is what makes it practicable for widespread use. The fact that the algorithm need not be kept secret means that makers can and have developed low-cost chip implementations of data encryption algorithms. These chips are widely available and integrated into a number of products. With the use of conventional encryption, the principal security problem is maintaining the secrecy of the key [5].

3. THE MAHAVIRACARYA RASILABDACHEDA MISRAVIBHAGA SUTRAM

In the history of mathematics in India and mathematical pedagogy, the 9th century popular mathematician from Karnataka state, India, Mahaviracarya occupies a significant place. He was the author of *Ganitha Saara Sangraha*. Many topics on algebra and geometry have been discussed in this book. Mahaviracarya gave a rule for separating the unknown dividend number, the quotient, and the divisor from their combined sum. This rule known as *"Rasilabdacheda misravibhaga sutram"* **[1].**

3.1 Rule

Any suitable optionally chosen number subtracted from the given combined sum happens to be the divisor. On dividing, by this divisor as increased by *one*, the remainder (left after subtracting the optionally chosen number from the given combined sum), the required quotient is arrived at. The very same remainder (above mentioned), as diminished by (this) quotient becomes the required dividend number [1].

We can summaries this rule as:

Combined sum	: x
Suitable optionally chosen no	: k
Divisor	: a
Dividend	: b

Quotient : *c*

x = a+b+c, then

$$a = x-k$$

$$c = \frac{k}{a+1}$$

$$b = k-c$$

3.2 An example

A certain unknown quantity is divided by a certain (other) unknown quantity. The quotient here as combined with the divisor and the dividend number is 53. What is that divisor, and quotient?

Here *x*=53; 45 chosen as *k*. Then from the above summary

$$a = x-k = 53-45 = 8$$

$$c = \frac{k}{a+1} = \frac{45}{8+1} = 5$$

$$b = k-c = 45-5 = 40$$

Therefore divisor (*a*) is 8, dividend (*b*) is 40 and quotient (*c*) is 5. If *k*=51 then divisor (*a*) is 2, dividend (*b*) is 34 and quotient (*c*) is 17. For different *k* values, we will get different *a*, *b*, *c* values.

4. A NEW METHOD FOR SYMMETRIC KEY CRYPTOGRAPHY

We can use the above rule for encrypt and decrypt the data. This rule has been used in conventional encryption method. The divisor (*a*) is taken as plain text, the quotient is taken as secret key (*c*) and combined sum (*x*) is taken as cipher text. When we decrypting the cipher text *x*, to get plain text *a* i.e. divisor in the above rule, we have to choose a number (*k*). But, for different *k* values, we will get different *a*, *b*, *c* values. So, to get correct *'a'* value here, we have to choose a suitable *k* value. Below, in decryption algorithm, a formula has been given how to find the suitable *k* value.

4.1 Encryption Method

$$b=a*c$$
$$x=a+b+c$$

x is the cipher text.

4.2 Decryption Method

$$k = \frac{c(x+1)}{c+1}$$
$$a = x-k$$

a is the plain text.

Maximum symmetric key cryptographic algorithms are either stream ciphers or block ciphers and not supporting both. These methods were implemented using either feistel structure or substitutions and permutations. In these algorithms decryption algorithm is reverse of the encryption algorithm.

This proposed method is entirely different from existing symmetric key cryptography algorithms. It can be used for stream ciphers and block ciphers. This method is using neither feistel structure nor substitutions and permutations structure. In this method decryption algorithm is not reverse to the encryption algorithm. It is a good mathematics application for symmetric key cryptography. . In this method secrete key and plain text block size lengths are variable, so it is very difficult to break the cipher. Since no techniques exist to prove that an encryption scheme is secure, the only test available is to see whether anyone can think of a way to break it [7]. The security of this method has to be tested in more detail for security attacks.

5. A SMALL EXAMPLE

5.1 Encryption

Consider the case

Plain text (*a*) = 33,
Secret key (*c*) = 56
then *b = a*c* = 33 * 56 = 1848

Cipher text (*x*) can be computed as

x = a+b+c = 33+1848+56 = 1937.

5.2 Decryption

Chosen number *k = c(x+1)/(c+1)*
= 56 (1937+1) / (56+1)
= 1904.

Plain text *a = x – k* = 1937 – 1904 = 33.

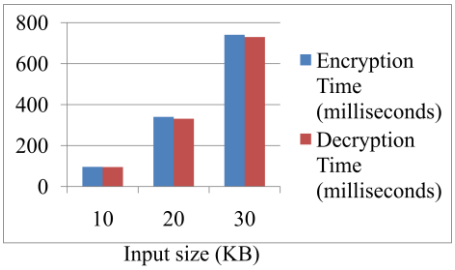
6. IMPLEMENTATION RESULTS

We implemented above method using java language. We have calculated the execution time of Encryption and Decryption algorithms for different sizes of text messages. For this experiment, we used Intel core2 Duo CPU T6670 @ 2.20 GHz with 2GB RAM, 32 bit operating System, Windows 7 Professional Service Pack 1, Net Beans IDE 7.4, Java 1.7.0_51.

Case 1: Execution time (milliseconds) of Encryption and Decryption of different data sizes using 90 bytes of Secret key for Stream Cipher. In Stream cipher encryption time is nearly equal to the decryption time. These times can be easily compared by observing the Table 1. and Graph-1.

Table 1. Execution time (milliseconds) for Stream Cipher

Input Size(KB)	Encryption Time (milliseconds)	Decryption Time (milliseconds)
10	96	95
20	340	331
30	741	730



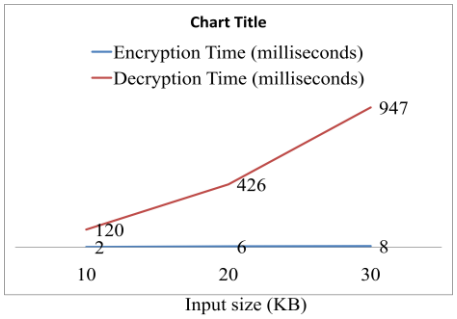
Graph-1: Comparison of encryption time and decryption time (milliseconds) for stream cipher

Case 2: Execution time (milliseconds) of encryption and decryption of different data sizes using 90 bytes of Secret

key for Block Cipher. Here, we have taken complete plain text as a single block. In this case decryption time is very high compared to the encryption time. These times can be easily compared by observing the Table 2. and Graph-2.

Table 2. Execution time (milliseconds) for Block Cipher (complete plaintext)

Input Size(KB)	Encryption Time (milliseconds)	Decryption Time (milliseconds)
10	2	120
20	6	426
30	8	947



Graph-2: Comparison of encryption time and decryption time (milliseconds) for block cipher

The above results show, that the encryption and decryption in stream cipher method is taking nearly same time. But, in case 2, the encryption time is very less than the decryption time and also less than the encryption time in stream cipher method. Decryption time is very high than the encryption time and also greater than the decryption time in stream cipher. If we take encryption and decryption as a unit, case 2 is taking less time than the case 1.

7. CONCLUSION

Mahaviracarya gave a mathematical formula for separating the unknown dividend number, the quotient, and the divisor from their combined sum is called *"Rasilabdacheda misravibhaga sutram"* (this is in Sanskrit language).This rule will give a good solution for cryptographic problems. From this rule a new conventional encryption algorithm was developed. This new symmetric encryption algorithm is very simple to understand and very easy to implement in any programming language. It is the first algorithm, which is used the mathematical formula instead off substitutions and transformations in conventional encryption algorithm. It can be used for both stream cipher and block cipher methods. In this algorithm secret key size is variable length so, it is very difficult to break the key as well as cipher text. This method has to be implemented for block ciphers. For block ciphers it's may give more security. If the security of this method proves to be sufficient, it can be used for symmetric key cryptography. The security of this method has to be tested in more detail. In future this algorithm can be tested for various block sizes of different data formats like audio, video and pictures with various key sizes and compare with existing symmetric and asymmetric key algorithms in terms of the execution time, power consumption and throughput etc… This algorithm can be tested for use in CryptDB.

8. REFERENCES

[1] Ganitha-Sara- Sangraha of Mahaviracarya by Rangacarya.M. Cosmo Publication New Delhi, India.

[2] Federal Information Processing Standards Publication 46-3, 1999 October 25, Announcing the DATA ENCRYPTION STANDARD(DES)

[3] Introduction to Modern Cryptography by Jonathan Katz and Yehuda Lindell.

[4] Cryptography and Network Security by Behrouz A. Forouzan.

[5] Cryptography and Network Security Principles and Practices by William Stallings.

[6] Discrete Mathematics and Its Applications 2nd Edition, Kenneth H. Rosen, Ph.D.

[7] A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, R.L. Rivest, A. Shamir, and L. Adleman.

[8] P.Princy, A Comparison of Symmetric Key Algorithms DES, AES, Blowfish, RC4, RC6: A Survey. International Journal of Computer Science & Engineering Technology (IJCSET) Vol.6 No.05 May 2015.

[9] A Symmetric Key Cryptographic Algorithm. 2010 International Journal of computer Applications (0975-8887) Vol. 1-No.15.

[10] Superiority of Blowfish Algorithm. International Journal of Advanced Research in Computer Science and Software Engineering. Vol. 2, Issue 9, September 2012. Pratap Chnadra Mandal.

[11] Secure Message Transmission with Low Computation. International Journal of Engineering and Innovative Technology (IJEIT) vol.1, Issue 6, June 2012. Dr.K.Venu Gopla Rao, Dr.P.Ramkumar.

[12] CryptDB: Protecting Confidentiality with Encrypted Query Processing. Raluca Ada Popa, Catherine M.S.Redfield, Nickolai Zeldovich, and Hari Balakrishnan MIT CSAIL.