Volume 3, No. 1, January 2012
Journal of Global Research in Computer Science
ISSN-2229-371X
RESEARCH PAPER
Available Online at www.jgrcs.info

NEW CONCEPT OF SYMMETRIC ENCRYPTION ALGORITHM A HYBRID APPROACH OF CAESAR CIPHER AND COLUMNAR TRANSPOSITION IN MULTI STAGES

Dharmendra Kumar Gupta*[1], Sumit kumar srivastava[2], Vedpal Singh[3]
[*1]M. Tech. (CSE) Student & Faculty of Computer Science & Engineering, IET Alwar, Rajsthan, INDIA
gupta.dharmendra0107@gmail.com, dharmendra.gupta0107@rediffmail.com
[2]M. Tech. (CSE) Student & Faculty of Computer Science & Engineering, D.B.I.T, Dehradun, (U.K.), INDIA
sumitsri15.007@gmail.com
[3]CSEDept. Dev Bhoomi Institute of Technology, Dehradun (U.K.), INDIA
vedpalsiet101@gmail.com

Abstract: Internet and networks applications are growing very fast, so the needs to protect such applications are increased. Encryption algorithms play a main role in information security systems. This work gives an insight into the new concept called hybrid approach of conventional encryption, which gives the concept of strong encryption of the data. The symmetric encryption also called conventional encryption or single key encryption was the only type of encryption is use prior to the development of public-key encryption. All the conventional encryption algorithms are very weak concept of encryption and brute-force attack and cryptanalysis attacks can easily determined the plain text. With the increasing use of the secure transmission of data and information over the internet, the need of strong encryption algorithm increasing day by day. In this work of encryption technique we present a new concept of conventional or symmetric encryption algorithm that hybrid two primitive (i.e. Caesar Cipher and Columnar Transposition) and weak approach of encryption algorithm in multi stages to make the new approach more secure and strong than the earlier concept. The core of this algorithm is the use of two different secret keys for the Caesar Cipher and Columnar Transposition respectively. The cryptanalysis attack can not determine the plaintext easily, brute-force attack required long time to obtain plaintext. The mechanism used for this new hybrid algorithm is, first encrypt the message by applying Caesar Cipher technique and again Transpose the encrypted message receive from the Caesar Cipher, this process repeat again and again as many times as number of digits in the secret key for the Caesar cipher.

INTRODUCTION

A Caesar cipher, also known as a Caesar's cipher, the shift cipher, Caesar's code or Caesar shift, is one of the simplest and most widely known encryption techniques. It is a type of substitution cipher in which each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet. For example, with a shift of 3, A would be replaced by D, B would become E, and so on. The method is named after Julius Caesar, who used it to communicate with his generals.

The general Caesar algorithm is –

$$C = E(p) = (p + k) \bmod (26)$$

where k takes on a value in the range 1 to 25. The decryption algorithm is simply

$$p = D(C) = (C - k) \bmod (26)$$

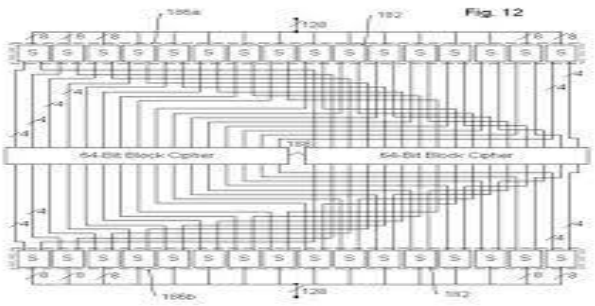

Figure. 1: Substitution Cipher

In a columnar transposition, the message is written out in rows of a fixed length, and then read out again column by column, and the columns are chosen in some scrambled order. A single columnar transposition could be attacked by guessing possible column lengths, writing the message out in its columns (but in the wrong order, as the key is not yet known), and then looking for possible anagrams. Thus to make it stronger, a double transposition was often used. This is simply a columnar transposition applied twice. The same key can be used for both transpositions, or two different keys can be used.

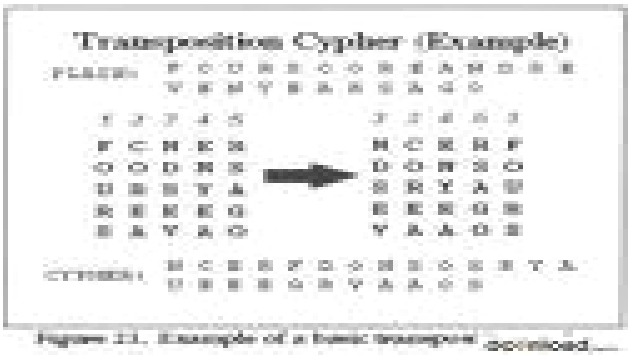

Figure.2: Simple Caesar Cipher

Columnar Transposition can be easily detected by the cryptanalyst by doing a frequency count. But in this new hybrid concept of conventional encryption technique, the Brute – Force Cryptanalysis is very difficult to detect the plaintext.

This new algorithm is hybrid of two most popular widely used symmetric encryption algorithms i.e. substitution algorithm (Caesar cipher) and transposition algorithm (Columnar transposition) in multi stage to make the new approach more secure and strong. The basic core of this algorithm is the use of two different secret keys for the

Caesar cipher and columnar transposition respectively. The cryptanalysis attack can not determine the plaintext easily, brute-force attack required long time to obtain plaintext.

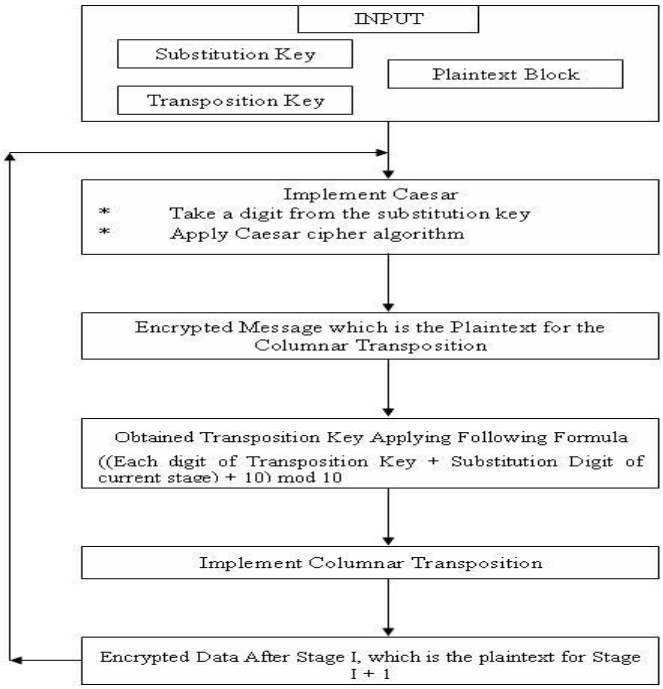

Figure 3: Hybrid Approach of Encryption Technique

RELATED WORK

To give more prospective about the performance of the hybrid algorithms, this section discusses the results obtained from other resources.

It was shown in [3] that Cryptography is the science of keeping data secure. There are two main types of cryptography that are used, symmetric and asymmetric. In this paper the focus upon possibility of hybrid these two encryption technique. Pretty Good Privacy (PGP) by Network Associates is an example of this. Symmetric and asymmetric cryptography both have advantages and disadvantages. PGP brings the best of each together and also works to minimize the disadvantages.

It was shown in [4] that a generic and simple conversion from weak asymmetric and symmetric encryption schemes into an asymmetric encryption scheme which is secure in a very strong sense indistinguishability against adaptive chosen cipher text attacks. In particular, this conversion can be applied efficiently to an asymmetric encryption scheme, like the ElGamal encryption scheme.

It was shown in [5] that present the implementation of a secure application for an academic institution with numerous services to both students and the faculty. This provides a technique of a new architecture for encrypting the database. The focus of this work mainly includes but is not limited to symmetric and public-key cryptography, authentication, key management, and digital signatures. The result of this work shows that what security features should implement in order to achieve a highly secured application and implementation of a stand alone system and still operates effectively.

It was shown in [6] Internet and networks applications are growing very fast, so the needs to protect such applications are increased. Encryption algorithms play a main role in information security systems. This work of study shows a comparatively study on various existing most common algorithms namely AES (Rijndael), DES, 3DES, RC2, Blowfish, and RC6. This work focus on the amount of computing resources such as CPU time, memory, and battery power. A comparison has been conducted for those encryption algorithms at different settings for each algorithm such as different sizes of data blocks, different data types, battery power consumption, different key size and encryption - decryption speed.

IMPLEMENTATION AND EXPERIMENTAL DESIGN OF HYBRID APPROACH OF CAESAR CIPHER AND COLUMNAR TRANSPOSITION IN MULTI STAGES

This study gives an insight into the concept called hybrid approach of conventional encryption, which gives the concept of strong encryption approach of the data. This study hybrid two most popular symmetric encryption algorithms i.e. substitution algorithm (Caesar cipher) and transposition algorithm (columnar transposition) in multi stage to make the new approach more secure and strong than the earlier concept. The core of this algorithm is the use of two different secret keys for the Caesar cipher and columnar transposition respectively. The cryptanalysis attack can not determine the plaintext easily; brute-force attack required very long time to obtain plaintext. A Caesar cipher is one of the simplest and most widely known encryption techniques. It is a type of substitution cipher in which each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet. For example, with a shift of 3, A would be replaced by D, B would become E, and so on. The method is named after Julius Caesar, who used it to communicate with his generals.

The encryption can also be represented using modular arithmetic by first transforming the letters into numbers, according to the scheme, A = 0, B = 1,..., Z = 25.Encryption of a letter x by a shift n can be described mathematically as,

$$E_n(x) = (x + n) \mod 26.$$

Decryption is performed similarly,

$$D_n(x) = (x - n) \mod 26.$$

In a columnar transposition, the message is written out in rows of a fixed length, and then read out again column by column, and the columns are chosen in some scrambled order. A single columnar transposition could be attacked by guessing possible column lengths, writing the message out in its columns (but in the wrong order, as the key is not yet known), and then looking for possible anagrams. Thus to make it stronger, a double transposition was often used. This is simply a columnar transposition applied twice. The same key can be used for both transpositions, or two different keys can be used. Simple Caesar Cipher or Columnar Transposition can be easily detected by the cryptanalyst by doing a frequency count. But in this new hybrid concept of conventional encryption technique, the Brute – Force Cryptanalysis is too difficult to detect the plaintext.

As these required two key for encryption of plaintext to produced cipher text, one is for substitution and other is for transposition. The number of stages in this algorithm depends upon the size of substitution key. For example if the secrete key for the substitution is 683594, then there is six stages because the numbers of digits is six. The recommended key secret key size for substitution is 20 digits. The substitution encryption take place according to the occurrence of digits, for example the first digit is 6, then in the first stage of substitution involve replacing each letter of alphabet with the letter standing six places further down the alphabet, with the help of the following formula.
Cipher Symbol = (Plaintext Symbol + Substitution Digits) mod 26

After the substitution take place for each digits of the secret key for Caesar cipher perform the columnar transposition encryption and thus each combination of Caesar cipher and columnar transposition produced the intermediate cipher which is plain text for the next stage.

At each stage, the columnar transposition encryption perform for the different secret key, the key can be obtained by adding digit of substitution at each stage in the every digits of original secret key of the transposition with the help of following formula.
((Each digit of Transposition Key + Substitution Digit of current stage) + 10) mod 10
Similarly decryption key can be obtained with the help of following formula -
((Each digit of Transposition Key - Substitution Digit of current stage) + 10) mod 10
The detail of this algorithm is explain here with the help of an example –

Example:

Suppose the given plaintext is -

"meet me after toga party"

Secret Keys –
* Secret key for Substitution – 683594
* Secret key for Transposition – 3142

Therefore the number of stages in this hybrid concept of symmetric encryption algorithm is six, because the numbers of digits in secret key for the substitution is six.

Stage First:

The key value for this stage is 6, so substitute each symbols of plain text with the symbol produced by the following equation.
Cipher symbol = (Position value of plain symbol + Key value of the stage) mod 26
= (Position value of m + 06) mod 26
= (13+06) mod 26
= 19 mod 26
= 19
Therefore the symbol at position 19 is S.

Similarly find the cipher symbol for each plain symbol in the given plaintext, now the intermediate cipher text after first stage of Caesar cipher substitution.

"SKKZ SK GLZKX ZUMG VGXZE"

Now apply the columnar transposition encryption on intermediate cipher text receive from the first stage of Caesar cipher. The original secret key for the columnar transposition is 3142 now find secret key for this stage of columnar transposition by adding 6 to each digit of original secret key for the columnar transposition with the help of following formula.
((Each digit of Transposition Key + Substitution Digit of current stage) + 10) mod 10
For digit 3 of 3142 –
= ((3 + 6) + 10) mod 10
= 9
For digit 1 of 3142 –
= ((1 + 6) + 10) mod 10
= 7
For digit 4 of 3142 –
= ((4 + 6) + 10) mod 10
= 0
For digit 2 of 3142 –
= ((2 + 6) + 10) mod 10
= 8
Now the new columnar transposition key for this stage is '9708'

9	7	0	8
S	K	K	Z
S	K	G	L
Z	K	X	Z
U	M	G	V
G	X	Z	E

"KGXGZKKKMXZLZVESSZUG"

This is the cipher text after first stage of hybrid approach of multistage symmetric encryption and also it is plain text for the next stage.

Stage Second:

The key value for this stage is 8, so substitute each symbols of plain text with the symbol produced by the following equation.
Cipher symbol = (Position value of plain symbol + Key value of the stage) mod 26
= (Position value of K + 08) mod 26
= (11+08) mod 26
= 19 mod 26
= 19
Therefore the symbol at position 19 is 'S'.
Similarly find the cipher symbol for each plain symbol in the given plaintext, now the intermediate cipher text after second stage of Caesar cipher substitution.

"SOFOHSSSUFHTHDMAAHCO"

Now apply the columnar transposition encryption on intermediate cipher text receive from the first stage of Caesar cipher. The original secret key for the columnar transposition is 3142 now find secret key for this stage of columnar transposition by adding 8 to each digit of original secret key for the columnar transposition with the help of following formula.
((Each digit of Transposition Key + Substitution Digit of current stage) + 10) mod 10
For digit 3 of 3142 –
= ((3 + 8) + 10) mod 10
= 1
For digit 1 of 3142 –

= ((1 + 8) + 10) mod 10
= 9

For digit 4 of 3142 –
= ((4 + 8) + 10) mod 10
= 2

For digit 2 of 3142 –
= ((2 + 8) + 10) mod 10
= 0

Now the new columnar transposition key for this stage is '1920'

1	9	2	0
S	O	F	O
H	S	S	S
U	F	H	T
H	D	M	A
A	H	C	O

"OSTAOSHUHAFSHMCOSFDH"

This is the cipher text after second stage of hybrid approach of multistage symmetric encryption and also it is plain text for the next stage.

Stage Third:

The key value for this stage is 3, so substitute each symbols of plain text with the symbol produced by the following equation.

Cipher symbol = (Position value of plain symbol + Key value of the stage) mod 26
= (Position value of O + 03) mod 26
= (15+03) mod 26
= 18 mod 26
= 18

Therefore the symbol at position 18 is R.

Similarly find the cipher symbol for each plain symbol in the given plaintext, now the intermediate cipher text after third stage of Caesar cipher substitution.

"RVWDRVKXKDIVKPFRVIGK"

Now apply the columnar transposition encryption on intermediate cipher text receive from the first stage of Caesar cipher. The original secret key for the columnar transposition is 3142 now find secret key for this stage of columnar transposition by adding 3 to each digit of original secret key for the columnar transposition with the help of following formula.

((Each digit of Transposition Key + Substitution Digit of current stage) + 10) mod 10

For digit 3 of 3142 –
= ((3 + 3) + 10) mod 10
= 6

For digit 1 of 3142 –
= ((1 + 3) + 10) mod 10
= 4

For digit 4 of 3142 –
= ((4 + 3) + 10) mod 10
= 7

For digit 2 of 3142 –
= ((2 + 3) + 10) mod 10
= 5

Now the new columnar transposition key for this stage is '6475'

"RVWDRVKXKDIVKPFRVIGK"

6	4	7	5
R	V	W	D
R	V	K	X
K	D	I	V
K	P	F	R
V	I	G	K

"VVDPIDXVRKRRKKVWKIFG"

This is the cipher text after third stage of hybrid approach of multistage symmetric encryption and also it is plain text for the next stage.

Stage Fourth:

The key value for this stage is 5, so substitute each symbols of plain text with the symbol produced by the following equation.

Cipher symbol=(Position value of plain symbol+Key value of the stage) mod 26
= (Position value of V + 05) mod 26
= (22+05) mod 26
= 27 mod 26
= 1

Therefore the symbol at position 1 is 'A'.

Similarly find the cipher symbol for each plain symbol in the given plaintext, now the intermediate cipher text after third stage of Caesar cipher substitution.

"AAIUNICAWPWWPPABPNKL"

Now apply the columnar transposition encryption on intermediate cipher text receive from the fourth stage of Caesar cipher. The original secret key for the columnar transposition is 3142 now find secret key for this stage of columnar transposition by adding 5 to each digit of original secret key for the columnar transposition with the help of following formula.

((Each digit of Transposition Key + Substitution Digit of current stage) + 10) mod 10

For digit 3 of 3142 –
= ((3 + 5) + 10) mod 10
= 8

For digit 1 of 3142 –
= ((1 + 5) + 10) mod 10
= 6

For digit 4 of 3142 –
= ((4 + 5) + 10) mod 10
= 9

For digit 2 of 3142 –
= ((2 + 5) + 10) mod 10
= 7

Now the new columnar transposition key for this stage is '8697'

"AAIUNICAWPWWPPABPNKL"

8	6	9	7
A	A	I	U
N	I	C	A
W	P	W	W
P	P	A	B
P	N	K	L

"AIPPNUAWBLANWPPICWAK"

This is the cipher text after fourth stage of hybrid approach of multistage symmetric encryption and also it is plain text for the next stage.

Stage Fifth:

The key value for this stage is 9, so substitute each symbols of plain text with the symbol produced by the following equation.

Cipher symbol=(Position value of plain symbol+Key value of the stage) mod 26

= (Position value of A + 09) mod 26

= (01+09) mod 26

= 10 mod 26

= 10

Therefore the symbol at position 10 is J.

Similarly find the cipher symbol for each plain symbol in the given plaintext, now the intermediate cipher text after third stage of Caesar cipher substitution.

"JRYYWDJFKUJWFYYRLFJT"

Now apply the columnar transposition encryption on intermediate cipher text receive from the fifth stage of Caesar cipher. The original secret key for the columnar transposition is 3142 now find secret key for this stage of columnar transposition by adding 9 to each digit of original secret key for the columnar transposition with the help of following formula.

((Each digit of Transposition Key + Substitution Digit of current stage) + 10) mod 10

For digit 3 of 3142 –

= ((3 + 9) + 10) mod 10

= 2

For digit 1 of 3142 –

= ((1 + 9) + 10) mod 10

= 0

For digit 4 of 3142 –

= ((4 + 9) + 10) mod 10

= 3

For digit 2 of 3142 –

= ((2 + 9) + 10) mod 10

= 1

Now the new columnar transposition key for this stage is '2031'

"JRYYWDJFKUJWFYYRLFJT"

2	0	3	1
J	R	Y	Y
W	D	J	F
K	U	J	W
F	Y	Y	R
L	F	J	T

"RDUYFYFWRTJWKFLYJJYJ"

This is the cipher text after fifth stage of hybrid approach of multistage symmetric encryption and also it is plain text for the next stage.

Stage Sixth:

The key value for this stage is 4, so substitute each symbols of plain text with the symbol produced by the following equation.

Cipher symbol=(Position value of plain symbol+Key value of the stage) mod 26

= (Position value of R + 04) mod 26

= (18+04) mod 26

= 22 mod 26

= 22

Therefore the symbol at position 22 is V.

Similarly find the cipher symbol for each plain symbol in the given plaintext, now the intermediate cipher text after sixth stage of Caesar cipher substitution.

"VHYCJCJAVXNAOJPCNNCN"

Now apply the columnar transposition encryption on intermediate cipher text receive from the sixth stage of Caesar cipher. The original secret key for the columnar transposition is 3142 now find secret key for this stage of columnar transposition by adding 4 to each digit of original secret key for the columnar transposition with the help of following formula.

((Each digit of Transposition Key + Substitution Digit of current stage) + 10) mod 10

For digit 3 of 3142 –

= ((3 + 4) + 10) mod 10

= 7

For digit 1 of 3142 –

= ((1 + 4) + 10) mod 10

= 5

For digit 4 of 3142 –

= ((4 + 4) + 10) mod 10

= 8

For digit 2 of 3142 –

= ((2 + 4) + 10) mod 10

= 6

Now the new columnar transposition key for this stage is '7586'

"VHYCJCJAVXNAOJPCNNCN"

7	5	8	6
V	H	Y	C
J	C	J	A
V	X	N	A
O	J	P	C
N	N	C	N

"HCXJNCAACNVJVONYJNPC"

This is the cipher text after final stage of hybrid approach of multistage symmetric encryption and also it is plain text for the next stage.

Key Size (Digits)	Number of Alternative Keys	Times Required at 1 Encryption /µs	Time Required for 50 Stages
2	!2 = 2	406112 µs	406112 x 50 = 20305600 µs
3	!3 = 6		
4	!4 = 24		
5	!5 = 120		
6	!6 = 720		
7	!7 = 5040		
8	!8 = 40320		
9	!9 = 362880		
Total	409112		

RESULT ANALYSIS

Brute – Force for Caesar Cipher:

If it is known that the obtained cipher text is produced by the Caesar cipher algorithm, then the brute – force cryptanalysis can be easily performed to obtain the plaintext.

Simply try all 25 possible keys to obtain the plaintext. The time required for the brute – force cryptanalysis for the Caesar cipher is few micro second (µs).

Brute – Force for Columnar Transposition:

Suppose that the columnar transposition encryption technique is performed for multiple stages to produce the cipher text, the brute force cryptanalysis can be performed on columnar transposition encryption to obtain the plaintext.

Key Size: Minimum - 2 Digits
Maximum - 9 Digits

Brute – Force Cryptanalysis for This New Concept of Symmetric Encryption Algorithm:

As the key concept of this algorithm is use of two encryption keys. One is use for Caesar cipher and other is used for columnar transposition, but the key for the Caesar cipher plays a significant role in columnar transposition encryption too.

Nos. of Digits for Caesar Cipher (A)	Nos. of Alternative Keys for Caesar Cipher (B)	Nos. of Alternative Keys for Columnar Transposition (C)	Total Nos. of Alternative Keys (D = B x C)	Time Required at 1 Encryption / µs (E)	Time Required at 10^6 Encryption / µs (F)
10	9^{10} = 3.4 x 10^9	4.1 x 10^5	1.4 x 10^{15}	43.75 Yrs	1400 Sec.
15	9^{15}= 2.1 x 10^{14}	4.1 x 10^5	8.4 x 10^{19}	2.625 x 10^{12} Yrs	2.625 x 10^6 Yrs.
20	9^{20}= 1.2 x 10^{19}	4.1 x 10^5	4.9 x 10^{24}	1.53 x 10^{17} Yrs	1.53 x 10^{11} Yrs.
25	9^{25}= 7.2 x 10^{23}	4.1 x 10^5	2.9 x 10^{29}	0.91 x 10^{22} Yrs	0.91 x 10^{16} Yrs.

CONCLUSIONS

As we know the symmetric encryption also referred to as conventional encryption or single key encryption, was the only type of encryption in use prior to the development of public – key encryption. The substitution and transposition encryption techniques were the most widely used symmetric encryption. The Caesar cipher was the earliest known use of substitution cipher. The Caesar cipher involves replacing each letter of plaintext with letter standing some places further down the alphabets. A brute - force cryptanalysis is easily performed, simply try all the 25 possible keys which takes few micro seconds. A different kind of encryption technique is achieved by performing some sort of permutation on the plaintext letters. This technique is referred to as a transposition cipher. The columnar encryption is more complex scheme is to write the message in a rectangle, row by row and read the message off, column by column but permute the order of the columns. The order of columns then becomes the key to the algorithm. A brute – force cryptanalysis also can be easily performed to decrypt the message, 50 stages columnar transposition can be detected in few seconds. This paper presents a strong approach of conventional encryption technique. The key concept of this algorithm is use of two encryption keys and that why it will be very difficult to performed brute – force cryptanalysis. As in the result analysis it will take very long time to decrypt the message. The attacker must should known the idea about the both keys to decrypt the message. The conventional encryption technique which is out dated technique these days. This paper presents the strong concept which tries to make popular symmetric encryption technique once again.

ACKNOWLEDGMENTS

The authors would like to thank anonymous reviewers for their valuable comments and suggestions that improve the presentation of this paper.

REFERENCES

[1]. William Stallings, "Cryptography and Network Security Principles and Practices 3rd Ed," Prentice Hall, 2003, PP. 11- 49.

[2]. Srinivasarao D, Sushma Rani N, Ch.Panchamukesh and S.Neelima "Analyzing the Superlative Symmetric Cryptographic Encryption Algorithm (ASCEA)" Journal of Global Research in Computer Science Volume 2, No. 7, July 2011.

[3]. Jessica J. Benz "PGP: A Hybrid Solution" SANS Institute InfoSec Reading Room.

[4]. Eiichiro Fujisaki and Tatsuaki Okamoto "Secure Integration of Asymmetric and Symmetric Encryption Schemes" NTT Laboratories 1-1 Hikarinooka, Yokosuka-shi, 239-0847 JAPAN.

[5]. Syed S. Rizvi, Aasia Riasat, Khaled M. Elleithy "Combining Private And Public Key Encryption Techniques For Providing Extreme Secure Environment For An Academic Institution Application" International Journal of Network Security & Its Application (IJNSA), Vol.2, No.1, January 2010.

[6]. Diaa Salama Abd Elminaam, Hatem Mohamed Abdual Kader, and Mohiy Mohamed Hadhoud "Evaluating the Performance of Symmetric Encryption Algorithms" International Journal of Network Security, Vol.10, No.3, PP.213-219, May 2010.

Short Biodata for the Author

Dharmendra K. Gupta is a M. Tech. student of Computer Science & Engineering at Teerthanker Mahaveer University, Moradabad. He Received a M.C.A. in Computer Application from Punjab Technical University, Jalandhar in 2009. Presently he is working as lecturer at Institute of Engineering & Technology, Alwar since august – 2010. He has research interests are in the areas of data & network security and programming language.

Sumit kumar srivastava is a M. Tech. student of Computer Science & Engineering at Teerthanker Mahaveer University, Moradabad. Presently he is working as Assistant professor. at Dev Bhoomi institution of Engineering & Technology Dehradun, Uttarakhand.

 **Er. Vedpal Singh** received the B.Tech (Computer Science and Engineering) degree from Shobhit Institute of Engineering and Technology, Saharanpur, Uttar Pradesh Technical University (UPTU), Lucknow (U.P.), INDIA, in 2009. Completed M.Tech (Computer Engineering) from University Institute of Engineering and Technology (Kurukshetra University Kuruukshetra), Haryana, INDIA in 2011. Currently, working as an Assistant Professor in Dev Bhoomi Institute of Technology (DBIT), Dehradun (U.K.), INDIA. My research areas are Smart Card Security Techniques, Biometrics Identification and Authentication Techniques and Cryptography and Aerospace Security.

