Volume 4, Issue 8, August 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

SMAVCT- An Amalgamtion of Substitution and Transposition Technique A Hybrid Multistage Cryptosystem Based on Affine, Vignere, and Columnar Transposition

[1]Preeta kamalia*, [2]Mohit khandelwal, [3]Neelam Sharm
[1]M. Tech. Research scholar of CSE Department, IET, Alwar, Rajasthan, India
[2]M. Tech. Associate professor of CSE Department, IET, Alwar, Rajasthan, India
[3]Ph.D Professor of ECE, Department, Delhi Technical University, India

Abstract— Today's world, the need to secured channel for information exchange is increased a lot to maintain privacy. The indispensable issues through cryptographic encryption techniques are acknowledge by information security to keep the raw data unchanged by the intruder over the unsecured channel. Any techniques used individually are proved to be weaker than hybrid approach in cryptography and can be intercepted by unauthorized access on an unsecured channel. The use of internet and network has lead to the development of a strong encryption algorithm in multistage. In this paper, we come up with an idea of encrypting primitive techniques to make it strong against cryptanalysis by combining Affine cipher, Vigenère cipher and Columnar Transposition in multistage depending on the key-size to prevent the plaintext by attacks using ASCII values as input text to encrypt the data. This work contributes not only to the fixed numbered values for encryption, but also we can cipher ASCII characters (Lower case, Upper case and digits) using SMAVCT. The procedure includes few stages by encrypting the plain-text using affine cipher followed by Vigenère cipher and columnar transposition using varying key. The number of steps depends on the length of the key size used during the encryption process. Every time the new key retrieved in each step will be used in successive steps of encryption schemes. The implementation of SMAVCT will be done using Java programming.

Keywords— Affine, ASCII, Cryptography, Encryption, Substitution, Transposition, Vigenère.

I. INTRODUCTION

The widen handling of digital media for information transmission through secure and unsecured channels exposes messages sent via networks to intruders or third parties. Encryption of messages in this modern age of technology becomes necessary for ensuring that data sent via communication channels become protected and made difficult for deciphering[1]. Enormous number of transfer of data and information takes place through internet, which is considered to be most efficient though it's definitely a public access medium. Therefore to counterpart this weakness, many researchers have come up with efficient algorithms to encrypt this information from plain text into ciphers [2].

In an encryption scheme, the message or information, referred to as plaintext, is encrypted using an encryption algorithm, turning it into an unreadable cipher text [3]. The idea of affine cipher is multiplication combined with addition, modulo m where m is an integer, to create more mixed up substitutions. The affine cipher is simply a special case more general mono-alphabetic substitution cipher. The key for the affine cipher consist of the ordered pair; say (*a*, *b*).In selecting the key, it is important to note the following restrictions; $a \neq 0$ and *b* must be chosen from among the integers 0,1,2,3… m-1 and $a \neq 0$ must be relatively prime to m(i.e. a should not have factors common with m). In general, affine cipher system in which plaintext letters are enciphered mathematically is:

$$C(k) = (ax + b) mod M \quad (1)$$

using function notation where x is numerical equivalent of plain text letter and M is the number of letters in the alphabet [4]. The decryption algorithm is simply:

$$D(k) = a^{-1}(x - b) mod M \quad (2)$$

where a^{-1} is modular multiplicative inverse of *a* modulo *M* is:

$$a^{-1} mod M = 1 \quad (3)$$

Alphabet	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
VALUE	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

5X+8	8	13	18	23	2	7	12	17	22	1	6	11	16	21	0	5	10	15	20	25	4	9	14	19	24	3
CIPHER	I	N	S	X	C	H	M	R	W	B	G	L	Q	V	A	F	K	P	U	Z	E	J	O	T	Y	D

Fig.1 Affine encryption technique

The Vigenère cipher consists of several Caesar ciphers in sequence with different shift values. In Caesar cipher each letter is shifted along some places. For example for a shift of 5 A will become f, b will map to g and so on. The Vigenère cipher uses sequence of different shift values and uses a table called tabula recta, Vigenère square, or Vigenère table. The table is a 26 * 26matrix in which the English alphabets are written 26 times in different rows representing the different possible shifts [5]. In general, Vigenère cipher system in which plaintext letters are enciphered mathematically is:

$$C(k) = \big(p(i) + k(i)\big) mod 26 \quad (4)$$

Using function notation where p (i) is the plain text at i^{th} position and k (i) is the key at i^{th} position.
The decryption algorithm is simply:

$$D(k) = \big(C(i) - k(i)\big) mod 26 \quad (5)$$

Blaise de Vigenère in the 16th century, proposed this algorithm to encrypt the plaintext using 26*26 squares as shown in Fig. 4.

In Columnar Transposition, the undisguised information i.e. the plaintext is written in rows of fixed length and are read columns wise in the increasing order of the key. A single columnar transposition is weak and the intruder can easily detect it as the cipher text received is only the interchange of places from plaintext. The brute-force cryptanalysts can easily detect the single columnar transposition by frequency count. To make it a strong technique the columnar transposition is done in multi stages and this paper implements multistage hybrid algorithms as shown in Fig. 2.

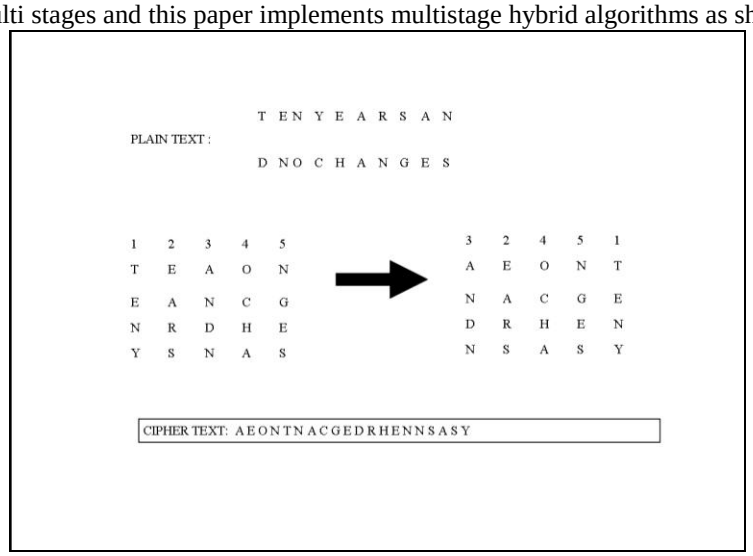

Fig. 2 Transposition ciphering technique

Procedure for singe columnar transposition cipher:
1. Chose a key of a fixed length
2. Write the plaintext row-by-row in rectangular form but with a fixed column which is equal to the chosen key.
3. Re-arrange the column into alphabetical column using the key as the determinant.
4. Read the message column-by-column.
5. The message read becomes the cipher text.

Suppose we want to encrypt the message “ORANGE PEEL” using a CT cipher with encryption key “feast”. Here is how we would proceed.

F	E	A	S	T
O	R	A	N	G
E	P	E	E	L

Now permute the columns so that the characters of the keyword are in alphabetical order.

A	E	F	S	T
A	R	O	N	G
E	P	E	E	L

Finally, concatenate the columns of the table obtained in step ii (excluding the keyword row) to obtain the cipher text: AERPOENEGL.

Many hybrid approaches are proposed to make it a strong technique for A-Z numbers by assigning them a place value range {0,1,…….25}.Quist-Aphesti kester proposed the method employs use of both Vigenère cipher and columnar transposition cipher in its encryption process. The cipher text will first be operated on using columnar transposition cipher. A chosen key out of random will initiate the transposition process. At the end of the process, the resulting cipher text then becomes a key for the Vigenère process. With the encryption process, a table of Vigenère cipher was created. The key is then used to operate on the message which is the plaintext to produce the final cipher text. This process will end up making the final cipher text more difficult to be broken using existing cryptanalysis processes. [6]

The greater character set and digits allow you to make your system more secure and more type of messages to be encrypted like passwords. So, we propose the algorithm for encrypting plain text for A-Z in upper case, a-z in lower case, and 0-9 digits using its ASCII value. The enhanced hybrid algorithm using SMAVCT is implemented using three basic cipher techniques affine, Vigenère, and columnar transposition in multistage to provide more security by increasing key domain.

ASCII TABLE FOR CONVERSION

Char	Dec	Hex	Oct	Char	Dec	Hex	Oct	Char	Dec	Hex	Oct
0	48	30	60	M	77	4D	115	i	105	69	151
1	49	31	61	N	78	4E	116	j	106	6A	152
2	50	32	62	O	79	4F	117	k	107	6B	153
3	51	33	63	P	80	50	120	l	108	6C	154
4	52	34	64	Q	81	51	121	m	109	6D	155
5	53	35	65	R	82	52	122	n	110	6E	156
6	54	36	66	S	83	53	123	o	111	6F	157
7	55	37	67	T	84	54	124	p	112	70	160
8	56	38	68	U	85	55	125	q	113	71	161
9	57	39	69	V	86	56	126	r	114	72	162
A	65	41	101	W	87	57	127	s	115	73	163
B	66	42	102	X	88	58	130	t	116	74	164
C	67	43	103	Y	89	59	131	u	117	75	165
D	68	44	104	Z	90	5A	132	v	118	76	166
E	69	45	105	a	97	61	141	w	119	77	167
F	70	46	106	b	98	62	142	x	120	78	170
G	71	47	107	c	99	63	143	y	121	79	171
H	72	48	110	d	100	64	144	z	122	7A	172
I	73	49	111	e	101	65	145				
J	74	4A	112	f	102	66	146				
K	75	4B	113	g	103	67	147				
L	76	4C	114	h	104	68	150				

Fig. 3 ASCII table for lowercase, uppercase, and digits

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Fig. 4 Vigenère table for upper case digits

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
a	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
b	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a
c	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b
d	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c
e	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d
f	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e
g	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f
h	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g
i	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h
j	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i
k	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j
l	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k
m	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l
n	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m
o	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n
p	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
q	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
r	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
s	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
t	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
u	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
v	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u
w	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
x	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w
y	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x
z	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y

Fig. 5 Vigenère table for lowercase digits

0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9	0
2	2	3	4	5	6	7	8	9	0	1
3	3	4	5	6	7	8	9	0	1	2
4	4	5	6	7	8	9	0	1	2	3
5	5	6	7	8	9	0	1	2	3	4
6	6	7	8	9	0	1	2	3	4	5
7	7	8	9	0	1	2	3	4	5	6
8	8	9	0	1	2	3	4	5	6	7
9	9	0	1	2	3	4	5	6	7	8

Fig. 6 Vigenère table for digits.

II. RELATED WORK

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

It is shown in [7] 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 is shown in [8] 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 comparative analysis on various existing and most common algorithms namely AES (Rijndael), DES, 3DES, RC2, Blowfish, and RC6. It focuses 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.

It is shown in [6], QUIST-APHETSI KESTER contribute to the general body of knowledge in the area of classical cryptography by developing a new hybrid way of encryption of plaintext. The cryptosystem performs its encryption by encrypting the plaintext using columnar transposition cipher and further using the cipher text to encrypt the plaintext again using Vigenère cipher.

A key of a fixed length was then chosen at random and entered into the system. The plaintext was then transformed row-by-row in rectangular form but with a fixed column which is equal to the chosen key. The columns were then re-arranged alphabetically using the key as the determinant. The final cipher text was then obtained by adding column-by column into a row. The cipher text then becomes a key for the Vigenère process. With the encryption process, a table of Vigenère cipher was created. The key is then used to operate on the message which is the plaintext to produce a cipher-text.

It is shown in [9], Dr. Fadhil proposed a hybrid combination of two public-key cryptosystem RSA and Knapsack, which offers extremely good security with less complexity and less time required for encryption- decryption process in compression with RSA and knapsack individually. The idea behind of this system is to use two stages of encryption. The enciphered text at the output of the first stage is as input message for the second stage. In the receiver, the enciphered transmitted message is decrypted using the RSA algorithm firstly and the knapsack algorithm secondly. Thus the decryption order is opposite to the encryption order. The steganography part includes hiding the secret message and digital signature after converting them to stream of bits.

It is proposed in [10], show a generic conversion from a very weak asymmetric encryption to an asymmetric encryption scheme which is secure in a very strong sense (IND-CCA in the random oracle model).

III. IMPLEMENTATION OF SMAVCT

The study proposed here provides the recognition about the concept of SMAVCT where basic substitution and transposition techniques are combined together in multiple stages to give strong encryption technique. SMAVCT stands for Substitution Multiple stages affine Vigenere columnar transposition. The basic techniques are easy to implement on any hardware system and results in better performance. SMAVCT studies hybrids three most popular techniques i.e. affine substitution cipher, vigenère encryption technique, and columnar transposition technique using ASCII values of the plain text which includes uppercase, lowercase, and digits. This complete encryption process continues in multistage which makes it stronger than earlier concept of hybrid cryptography. The main focus is we use different keys for different encryption and key-stages depend on the key-size. It becomes difficult for the cryptanalyst to determine the plain text easily. The technique becomes stronger as ASCII value is different from the fixed place values which are encrypted in multiple stages. The upper case and lower case alphabets values in ASCII range are different so it becomes more secure and efficient to use in passwords. The affine substitution cipher is monoalphabetic substitution where (a, b) are selected in such a way that they are relatively prime to each other. Each letter in the plaintext is mapped to its equivalent numerical value for encryption using Eq. (1). A modular arithmetic is performed on the integer values of the plaintext to encrypt which later results in the cipher text. Similarly, decryption technique is performed using Eq. (2) to convert the cipher text thus received so far.

The Vigenère cipher is polyalphabetic substitution cipher used to encrypt for alphabets 26*26 square matrix tables is defined to encrypt the plain text as shown in Fig. 4, 5. Vigenere table consist of row and columns for key and plaintext respectively. The keyword concatenated with the plain text gives the corresponding cipher text for the alphabets. Vigenère cipher table for alphabets is also designed in this paper for digits as shown in Fig.6. The weakness of monoalphabetic substitution is overcome using this technique by a combination of affine and vigenère making it a hybrid approach.

The transposition technique is basically a permutation done in a different way on plaintext letters so it is useful than substitution cipher which involves the process of replacing one alphabet with other. In columnar transposition process the plain text is written row-wise in a rectangle of defined key-size and the message is read column wise in increasing order. To increase more complexity this basic technique is done in multiple stages to make the plain text secure and become difficult for the intruder to attack. This strength of transposition is conjugated with combined affine and vigenère to make a strong cipher text which cryptanalyst cannot decipher easily. So, it is difficult for the cryptanalyst or brute-force attack on plaintext becomes too difficult to decipher it.

Example: Hybrid Algorithm using ASCII values in Multistage

Now take two values for affine (a, b) such that they are relatively prime to the plain text and $a \neq 0$. Refer Fig. [3] for ASCII values of the plain text and apply $mod65, mod97$ or $mod48$ for upper case, lower case, and digits respectively. Then calculate $(ax + b) mod26$ or $(ax + b) mod10$ on the digits received so far. Add 65, 97 or 48 to the calculated value if the plain text is in uppercase, lowercase or digits respectively.

As this requires three different keys for encryption of plaintext, so the number of stages depends on the Vigenère key used. For example if the secret key for Vigenère is "HER". Then total number of stages is 3 as number of digits is three. The transposition encryption takes place according to the occurrence of Vigenère key by adding the place value of the key to the transposition key digits to get a new key.

After the affine cipher takes place on ASCII value for each character performs the Vigenère encryption by referring Fig. 4, 5, or 6 as required for uppercase, lower case or digits respectively. The concatenated block for the respective cipher text received from the affine cipher and 1stkey letter of vigenère will be cipher text for the next stage.

After the vigenère process columnar transposition is applied on the text, the columnar transposition performs different secret key at each stage by adding the vigenère digit of the current stage to the transposition key to get the new key for this stage and performing modulo function with the help of the given formula. The process of affine to vigenère followed by transposition continues till the vigenère key length becomes empty. The place value of the vigenère key is added to the digit of transposition to obtain the new key and applying modulo function. The transposition cipher thus obtained is written in increasing order of the key value to obtain the cipher text.

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

The flowchart for SMAVCT describes about the procedure for hybrid encryption using affine, vigenère, and columnar transposition as shown in Fig. 10.

The plain text is read as PT, affine key as A and B, vigenère key as K, and transposition key as P. The encryption process number of stages depends on vigenère key so it continues until it becomes null. Then calculate ASCII value of the plain text and check whether the value is in uppercase, lowercase, or digits. After retrieving the cipher text as CT calculate place value of vigenère key and add to transposition key digits to get a new transposition key. Further, apply columnar transposition on the CT. Now decrease the vigenère key and the cipher text will become the plain text for the new stage.

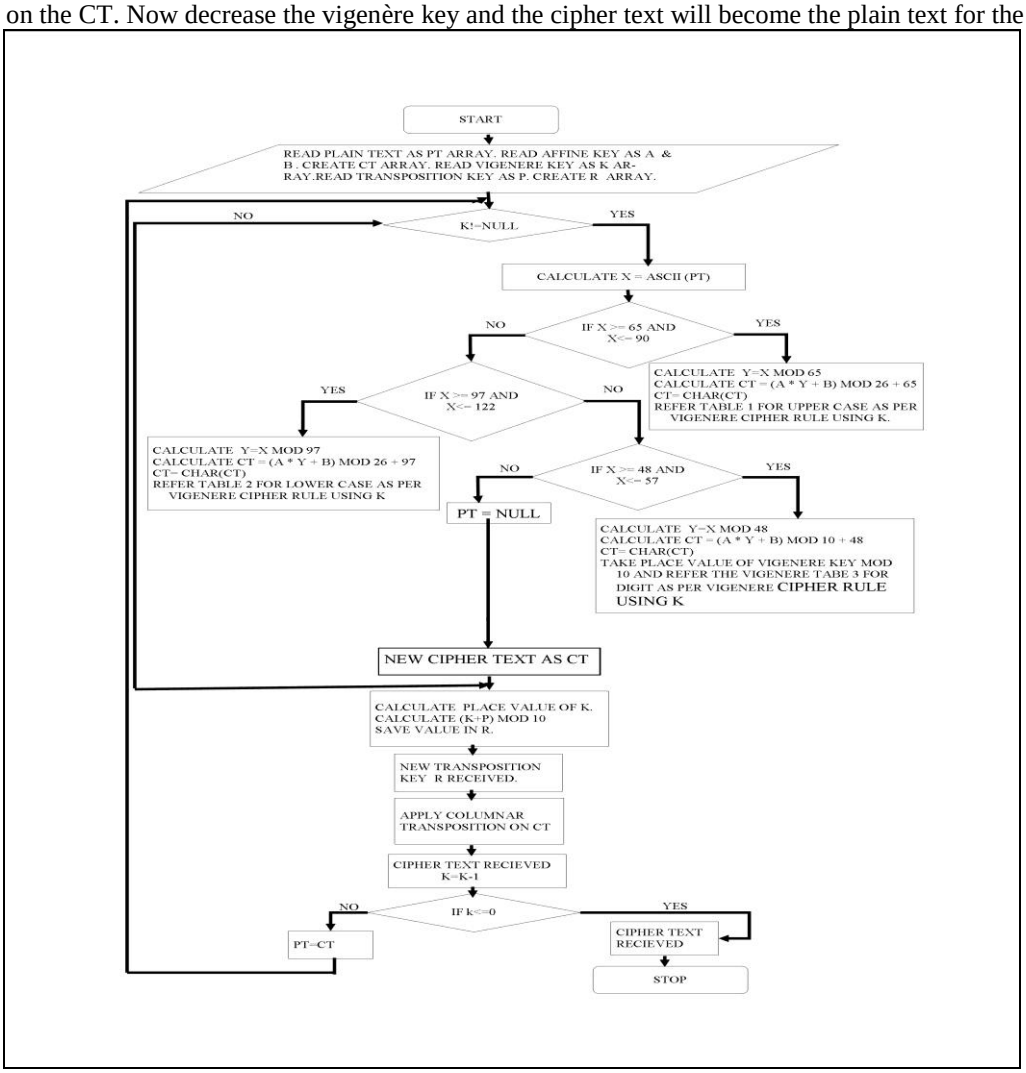

Fig. 10 Vigenère table for lowercase digits

The flowchart is described in stepwise below as:

1. START
2. READ A CHARACTER FROM PLAIN TEXT AS PT
3. X ← ASCII (CH)
4. IF X >= 65 AND X<= 90 THEN
5. Y ← X MOD 65
6. ELSE IF X >= 97 AND X<= 122 THEN
7. Y ← X MOD 97
8. OTHERWISE
9. Y ← X MOD 48
10. IF (X >= 65 AND X<= 90) THEN
11. CALCULATE CT = (A x Y + B) MOD 26 + 65
12. ELSE IF (X >= 97 AND X<= 122) THEN
11. CALCULATE CT = (A x Y + B) MOD 26 + 97
12. OTHERWISE
13. CALCULATE CT = (A x Y + B) MOD 10 + 48
14. REPEAT STEP 2 TO 13 UNTIL NOT EOF
15. READ A CHARACTER FROM PLAIN RECEIVED FROM AFFINE CIPHER AS PT
16. IF PT IS >=65 AND PT<=90 THEN

REFER TABLE 1 FOR UPPER CASE AS PER VIGENERE CIPHER RULE

17. ELSE IF PT IS >=97 AND PT<=122 THEN
    REFER TABLE 2 FOR LOWER CASE AS PER VIGENERE CIPHER RULE

OTHERWISE

18. TAKE PLACE VALUE OF VIGENERE KEY MOD 10 AND REFER THE VIGENERE TABE 3 FOR DIGIT AS PER VIGENERE CIPHER RULE
19. REPEAT STEP 15 TO 19 UNTIL NOT EOF
20. READ A CHARACTER FROM PLAIN RECEIVED FROM VIGENERE TEXT AS PT
21. CALCULATE PLACE VALUE OF VIGENERE KEY
22. READ A KEY USED IN TRANSPOSITION AS KEY3
23. ADD STEP 22 AND STEP 23 MOD10
24. FILL THE PT FROM LEFT TO RIGHT IN THE KEY TABLE
25. READ THE CHARACTERS ROW-WISE IN INCREASING ORDER OF THE KEY.
26. IF VIGENERE KEY ≠ NULL REPEAT STEP 2 TO 26
27. ELSE CIPHER TEXT IS RECEIVED.

The summarized process for SMAVCT is mentioned below as shown Fig. 11.

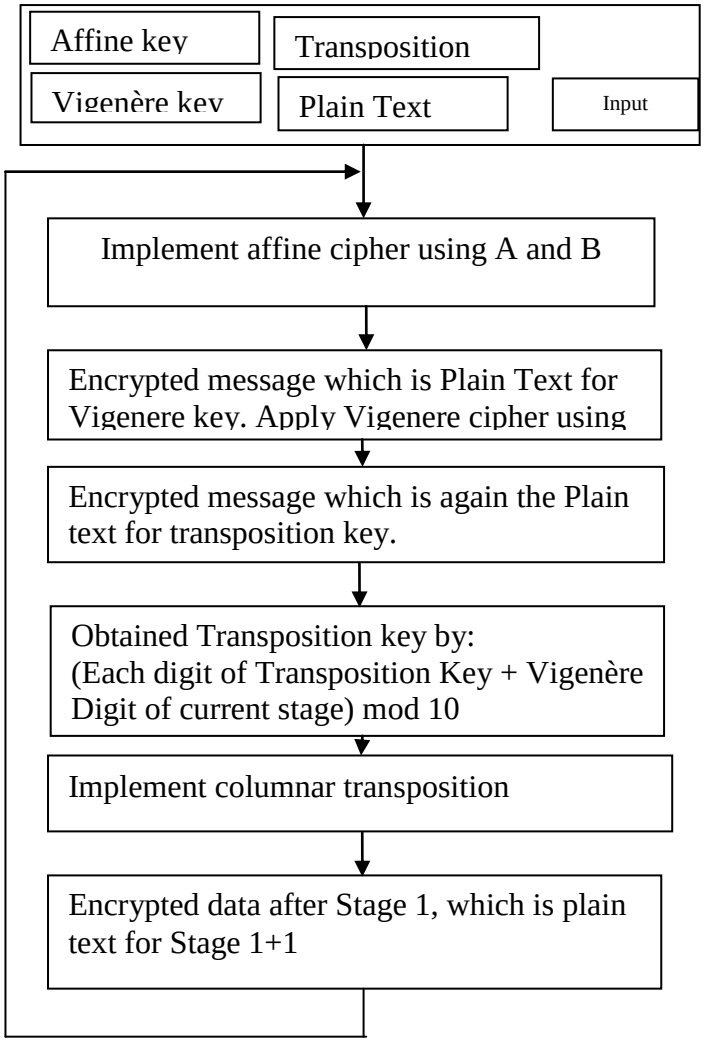

Fig. 11: Summarized flowchart for SMAVCT

Example:
Key for Affine - a = 5, b = 8
Key for Vigenère – HER
Key for Transposition – 8326

Therefore, the number of stages in SMAVCT algorithm is three, because the key-size of vigenère is three.
Plain Text = "Encrypt 7 Step"
Total stage = Length of (HER) = 3
Stage First
Affine:

Step1:

Plaintext	**E**	**n**	**c**	**r**	**y**	**p**	**t**	**7**	**S**	**t**	**e**	**p**
ASCII value	69	110	99	114	121	112	116	55	83	116	101	112
Mod(65) / mod(97) / mod(48)	4	13	2	17	24	15	19	7	18	19	4	15
5x+8	28	73	18	93	128	83	103	43	98	103	28	83
y=(5x+8) mod26 y=(5x+8)mod10	2	21	18	15	24	5	25	3	20	25	2	5
y+65/ y+97/y+ 48	67	118	115	112	121	102	122	51	85	122	99	102
Cipher text	C	v	s	p	y	f	z	3	U	z	c	f

Plain text for Vigenère "Cvspyfz3Uzcf"

Step2:

Vigenère Cipher	C	v	s	p	y	f	z	3	U	z	c	f
Key for Vigenère	H	H	H	H	H	H	H	H	H	H	H	H
New cipher	K	d	a	x	g	n	h	0	C	h	k	n

Plain text for transposition "Kdaxgnh0Chkn"

Step 3:
Key = 8326, place value of H=7
New key:

a. (8+7) mod 10=5
b. (3+7) mod 10=0
c. (2+7) mod 10=9
d. (6+7) mod 10=3

Key = 5093

5	**0**	**9**	**3**
K	d	a	x
g	n	h	0
C	h	k	n

Plain text for the stage 2 ""dnhx0nKgCahk"

New plain text for next stage dnhx0nKgCahk is received from the stage 1 which describes the sequence of the encryption performed on the plain text. After the transposition cipher applied in step 3 of stage 1, we will check the next vigenère key and perform the same sequence of operation in stage second. The key for this stage is E and the place value of E is 4 which is used in transposition to add up with key of transposition to get new key. The process continues till the key ends.

Stage Second
Affine
Step 1:

Plaintext	**d**	**n**	**h**	**x**	**0**	**n**	**K**	**g**	**C**	**a**	**h**	**k**
ASCII value	100	110	104	120	48	110	75	103	67	97	104	107
Mod(65)/ mod(97)/ mod(48)	3	13	7	23	0	13	10	6	2	0	7	10
5x+8	23	73	43	123	8	73	58	38	18	8	43	58

y=(5x+8) mod26 y=(5x+8)mod10	23	21	17	19	8	21	6	12	18	8	17	6
y+65/ y+97/y+48	120	118	114	116	56	118	71	109	83	105	114	103
Cipher text	x	v	r	t	8	v	G	m	S	i	r	G

Plain text for vigenère: "xvrt8vGmSirg"

Step 2:

Vigenère Cipher	x	v	r	t	8	v	G	m	S	i	r	g
Key for Vigenère	E	E	E	E	E	E	E	E	E	E	E	E
New cipher	c	a	w	y	2	a	L	r	X	n	w	l

Plain text for transposition "cawy2aLrXnwl"

Step3:
Key = 8326, place value of E=4
New key:

a. (8+4) mod 10=2
b. (3+4) mod 10=7
c. (2+4) mod 10=6
d. (6+4) mod 10=0

Key = 2760

2	**7**	**6**	**0**
c	a	w	y
2	a	L	r
X	n	w	l

Plain text for Transposition "yrlc2XwLwaan"

The key for this stage is R whose place value is 17 which is added to transposition key to get new key. The plain text retrieved in stage second is plain text for stage third.

Stage Third
Affine

Step1:

Plaintext	**y**	**r**	**l**	**c**	**2**	**X**	**w**	**L**	**w**	**a**	**a**	**n**
ASCII value	121	114	108	99	50	88	119	76	119	97	97	110
Mod(65) / mod(97) / mod(48)	24	17	11	2	2	23	22	11	22	0	0	13
5x+8	128	93	63	18	18	123	118	63	118	8	8	73
y=(5x+8) mod26 y=(5x+8)mod10	24	15	11	18	8	19	11	11	11	8	8	21
y+65/ y+97/y+48	121	112	108	115	56	84	108	76	108	105	105	118
Cipher text	y	p	l	s	8	T	l	L	l	i	i	v

Plain text for vigenère: "ypls8TlLliiv"

Step 2:

Vigenère Cipher	y	p	l	s	8	T	l	L	l	i	i	v
Key for Vigenère	R	R	R	R	R	R	R	R	R	R	R	R
New cipher	q	h	d	k	5	L	d	D	d	a	a	n

Plain text for transposition "qhdk5LdDdaan"

Step 3:
Key = 8326, place value of R=17
New key:

a. (8+17) mod 10=5
b. (3+17) mod 10=0
c. (2+17) mod 10=9
d. (6+17) mod 10=3

Key = 5093

5	**0**	**9**	**3**
q	h	d	k
5	L	d	D
d	a	a	n

Final cipher text is: "hLakDnq5ddda"

This is the cipher text after final stage of hybrid approach of multistage substitution and transposition encryption using SMAVCT on ASCII values of uppercase, lowercase, and digits.

IV. RESULT ANALYSIS

Brute force attack for affine cipher:

There exists many possible combinations for keys a and b and they must not be relatively prime to each other as they are input in affine cipher. Therefore, brute-force attack is not feasible but when we perform frequency analysis on the cipher text will result in many possible outcomes to decrypt the message in few microseconds (µs).

Brute force attack for vigenère cipher:

If suppose there are four subkeys, and the most likely subkey for the first, second, third, and fourth are five , two, one and five respectively. Then the possible combination to break the vigenère cipher is 5*2*1*5. If the vigenère key becomes larger then it is more difficult break the cipher text as shown in Fig. 8.

Brute force attack for double columnar cipher:

Suppose that the double columnar transposition is performed on multiple stages to obtain the ciphered text, the brute force cryptanalysis can be performed to transform the encrypted text to plain text. The maximum key-size for transposition can be 9 digits whereas the minimum can be 2 digits for the key-size as shown in Fig. 7.

Brute force attack for hybrid SMAVCT

As the key concept of SMAVCT proposes three algorithms, it uses three different subkeys for each encryption technique. One key for affine encryption technique, other for vigenère ciphering process, and the last one for double columnar transposition process are used. But the key for vigenère process plays a significant role for encryption as the total number of stages depends on the key-size of vigenère as shown in Fig. 9.

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		

Fig. 7: Time required for columnar transposition

Key Size (Digits)	Number of Alternative Keys	Nos. of alternative keys for Vigenère	Time Required at 1 Encryption /µs For 10 key-size
1	$^{26}C_1 = 26$	26	8.2* 10^6 Sec
2	$^{26}C_2=325$	26*325= 8450	
3	$^{26}C_3= 2600$	8450*2600=2.1*10^7	
4	$^{26}C_4= 14950$	(2.1*10^7)*14950 = 3.2*10^{11}	
5	$^{26}C_5= 65780$	(3.2*10^{11})*65780 = 2.16*10^{16}	
10	$^{26}C_{10}=5311735$	8.2*10^{46}	

Fig. 8: Time required for vigenère encryption process

No. of Alternative Keys for Affine (J)	No. of Digits for vigenère Cipher (A)	No. of Alternative Keys for Vigenère Cipher (B)	No. of Alternative Keys for Columnar Transposition (C)	Total Nos. of Alternative Keys (D = B x C x J)	Time Required at 1 Encryption / µs (E)	Time Required at 10^6 Encryption / µs (F)
36	5	2.16*10^{16}	4.1x10^5	3.18 x 10^{23}	1.01*10^{21} Yrs	1.01*10^{15} Sec
36	10	8.2*10^{46}	4.1x10^5	1.2 x 10^{54}	3.8*10^{40} Yrs	3.8* 10^{34} Sec
36	15	4.7*10^{51}	4.1x10^5	6.9x 10^{58}	2.18*10^{45} Yrs	2.18*10^{39} Sec
36	20	1.74*10^{82}	4.1x10^5	2.6x 10^{89}	8.2*10^{75} Yrs	8.2* 10^{61} Sec

Fig. 9: Time required for SMAVCT approach

V. CONCLUSIONS

Prior to the development public key encryption technique, the only symmetric encryption technique which is also called as single key encryption or conventional were used. The most common and widely used techniques are substitution and transposition ciphering. The affine cipher is very insecure individually and easy to break using brute force attack. The substitution cipher technique was implemented in vigenère cipher which is an enhanced ceaser cipher in multiple stages. The transposition technique is performing permutation operation the plain text to obtain the encrypted text. The transposition technique is a complex scheme as it is written row by row and read column –wise which is further the key to algorithm. The brute force algorithm can easily be performed on vigenère and transposition to decrypt the message. The entire scheme is prone to exhaustive search and can be decrypted in less time. This paper presents a new scheme

named SMAVCT which proposes a hybrid approach of the conventional encryption method. The key concept of SMAVCT proposes three hybrid structures of affine, vigenère, and columnar transposition and the number of stages depend upon the key length of vigenère cipher used. The hybrid approach makes it very difficult for the brute force attack. As in result it takes a long time to decrypt the message. The simple techniques are easy to implement on hardware so this paper helps in using simple conventional techniques for a very strong encryption process.

ACKNOWLEDGMENT

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

I would like to express my very great appreciation to Dr. Neelam Sharma for her valuable and constructive suggestions during the planning and development of this research work. Her willingness to give her time so generously has been very much appreciated.

REFERENCES

[1] Kester, Quist-Aphetsi. "A cryptosystem based on Vi-genère cipher with varying key." International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) [Online], 1.10 (2012): pp: 108-113. Web. 16 Jan. 2013

[2] Kester, Quist- Aphetsi., & Danquah, Paul. (2012). A novel cryptographic key technique. In Adaptive Science & Technology (ICAST), 2012 IEEE 4th In-ternational Conference on (pp. 70-73).

[3] (2004) The Wikipedia website.[online]. Available: http://www.en.wikipedia.org/wiki/encryption#cite_ref-golreich_2-1 goldreich,oded.foundations of cryptography:volome2,basic applications. Vol.2. Cambridge university press.

[4] (2011) The springer website.[online]. Available: http://link.springer.com/chapter/10.1007%2F978-3-642-25327-0_17, pp: 185-199.

[5] Alpha-qwerty cipher, "Advanced computing: An extended vigenère cipher," http://airccse.org/journal/acij/papers/0512Acij11.pdf, vol.3, No.3, May 2012

[6] Quist-Aphetsi kester, "A Hybrid cryptosystem based on Vigenere cipher and columnar transposition cipher," Ghana technology university college, Accra North, Ghana, January 2013.

[7] Jessica J. Benz, (2001) A Sans Institute infosec reading room. [online] "PGP: A Hybrid Solution".

[8] 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.

[9] Dr. Fadhil Salman Abed, "A Proposed Method of Information hiding based on Hybrid Cryptography and Steganogrpahy, IJAIEM - ISSN 2319 – 4847, Volume 2, ISSUE 4, APRIL 2013.

[10] Eiichiro Fujisaki and Tatsuaki Okamoto, "Secure Integration of Asymmetric and Symmetric Encryption Schemes," springer verlab NTT Laboratories, 1999, pp. 537-554.

[11] William Stallings, *Cryptography and Network Security*, 5th edition, Pearson Edu 2006, NewYork, Prentice Hall, 2011.

[12] Kavit Meral Mehta, Saksham Sharma, " Encryption using Affine and one time Pad," VIT university, Tamil Nadu, India, June 2013.

[13] Pelzl & Paar (2010). Understanding Cryptography. Berlin: Springer-Verlag. p. 30.

[14] Anderson,J."A unification of computer and network security concepts", *Proc.IEEE Symp. On Security and Privacy*, 1997, 65-71.

Short Bio-data for the author

Preeta kamalia is a M. Tech. student of Computer Science & Engineering at Institute of Engineering and Technology, Alwar. She Received a B.Tech in Computer Science department from Institute of Technology and Management, Gorakhpur, Uttar Pradesh, India in 2008.
She has research interests are in the areas of data & network security and programming language.

Mohit khandelwal received the B.E. degree in Information technology from the University of Rajasthan, Jaipur and M.E.degree in software system from the Birla Institute of Technology and Science, Pilani in 2007.
Since 2007, he has been an Associate Professor of Computer Science & Engineering, IET Alwar, India. He has guided eight M.tech students for their final thesis and has published more than 15 papers in various national and international journals. His research interests include Data and Network Security, Quality of Service issues of Routing Algorithms in Mobile Adhoc Networks, and Complexity analysis of Algorithms. He is taking seminars and workshops on the recent trends in CS/IT industry of B. Tech Students.

Neelam Sharma passed her B.E. (EC) with honors from Thapar Institute of Engineering & Technology, Patiala. She is a gold medallist of GNDU, Amritsar and has been teaching B.Tech. / M.Tech. classes since 1985.

She did her M.Tech and Ph.D. from UPTU, Lucknow. She has guided 04 Ph.D's and many M.Tech Dissertations & B.Tech projects. The areas of her special interest are Computer Architecture, CAD, VHDL, VLSI Technology, VLSI Design and Nano Technology. She has published and presented more than 57 papers in various Journals and conferences. She has four books to her credit. She has been sanctioned many Research Projects by A.I.C.T.E. and M.H.R.D worth 1.00 Cr. She has represented Institute of Engineering and Technology as Principal successfully for NBA presentation and preparation twice. World Bank project report has been prepared under her guidance & sanction approved worth 4.00 Crore is done by NPIU. Presently she is working as Director Delhi Technical Campus, G.Noida, an Institute affiliated to GGS Indraprastha University, N. Delhi.

