International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 2 Issue 3, March - 2013

English Encryption Technique Using Multilanguage

M.Rajendiran[1], K.Selvam[2] , N.Ranjith Kumar[3], T.Venkatesh[4]

[1]Asst. Professor, Chettinad College of Engineering & Technology,Tamilnadu,India.

[2]Student, Chettinad College of Engineering & Technology,Tamilnadu,India.

[3]Student, Chettinad College of Engineering & Technology,Tamilnadu,India.

[4]Student, Chettinad College of Engineering & Technology,Tamilnadu,India.

***Abstract*—Cryptosystem is a process of secret writing and it is a secure communication system. In this system there are certain rules and regulations to encrypt and decrypt the plaintext. These rules and regulations are in the form of algorithm to achieve the crypto (secrecy) process. To achieve this secrecy there is a Multilanguage Two Dimensional Array Substitution method (MTDAS) [2] where single 2D array is used for getting ciphertext. This system has a character repetition, so frequency analysis is possible to obtain the plaintext. Thus here we proposed a new method called English Encryption Technique Using Multilanguage (EETUM) which involves more character in ciphertext due to encryption of quotient (Q) value along with the reminder value (R) in the algorithm. Thus it proves more confidentiality and secure. The numerals are encrypted using our substitution technique.**

***Keywords*- Multilanguage, MTDAS, EETUM, Quotient (Q) value, Numerals.**

I.INTRODUCTION

It is an interesting fact that in a Cryptosystem, increase of secrecy in the plaintext ends in complexity in achieving the cipher text. The outcome of the cipher text faces great challenge in the cryptanalysis. The "classical cryptography" [3] was found in 1600BC by the **Tamil people**. Especially Thiruvalluvar in **Tirukkural** used the "porulkoal" for identifying the meaning of the words used in his poem. It is quite interesting that without knowing the porulkoal it is difficult to understand the Tirukkural.

In 1500BC **Egyptians** used the cryptographic technique by using their symbolic representation. During the period of 500BC **Hebrews** introduced the zigzag way of writing for achieving secrecy. In 486BC **Spartans** introduced the transposition ciphers which were written in a strip of leather and it is rolled off in a cylinder to retrieve the message.

In "medieval cryptography" (60-70 BC) there comes, Caesar cryptography where substitution method is used in plaintext. In the later period of 20th century there comes a "modern cryptography". Thus this paves a way for the various security systems such as Data Encryption Standard (DES) [3], Triple DES and Advanced Encryption Standard (AES) [3]. But all were ASCII based cryptography technique. In ASCII only 128 characters are available so its prediction is easy, by the way of Brute force attack and frequency analysis.

In "Visual Cryptography" [6] the optical illusion is a technique which is used in pictures to hide information along with the picture. The picture appears normal if we just have a glance of look at it. But it contains information if we see keenly onto the picture. Though all these algorithms are existing there are many cryptanalysis techniques to break the algorithm in the fast emerging computerized world. Thus our algorithm EETUM proves better security in logical prediction.

II.EXISTING METHOD

In Multilanguage Encryption Technique (MULET) [1] and MTDAS technique, the Unicode value is obtained for each Multilanguage plaintext character. The constant value is assigned for mapping (M). Then the Unicode value [4] is divided by mapping constant (M) which gives the quotient (Q) and reminder (R) value. The reminder values are grouped depending on the dimensional array. The serial numbering is given to the grouped values and it is separated accordingly to the odd and even numbers.

For instance, consider the below given table I, II and III of encryption, 2D mapping array and decryption of MTDAS where the value for M=3 is assigned. The Unicode value for G is 71 so by dividing 71 by 3 we get Q=23 and R=2 similarly if we consider for the letter O the Unicode is 79 and if divided by 3 we get Q=26 and R=1. Then the reminder values (2, 1) are grouped. This assigns serial values of 1 so it is considered as an odd parity. In the mapping array table, if it is an odd parity then (row, column) should be considered. For even parity (column, row) should be considered. But in this encryption technique only 3*3=9 characters are available so there is a possibility for frequency analysis since only 9 characters get repeated in the ciphertext.

The obtained ciphertext is a block cipher and the quotient value here is a key value, so it has to be sent separately using Steganography method. But in EETUM there is no need for another algorithm to process Q value. The Q value is used in encryption itself. Thus there is a less possibility for intruder to get the quotient values along with ciphertext.

TABLE I

MTDAS ENCRYPTION

Plaintext	G O	D I	S G	R E	A T
Unicode	71 79	68 73	83 71	82 69	65 84
M	3	3	3	3	3
Q	23 26	22 24	27 23	27 23	21 28
R	2 1	2 1	2 2	1 0	2 0
RG	2,1	2,1	2,2	1,0	2,0
SN	1	2	3	4	5
PA	ODD	EVEN	ODD	EVEN	ODD
RC	R,C	C,R	R,C	C,R	R,C
BC	आ	ई	ट	அ	इ

M=Mapping constant, Q=Quotient, R=Reminder

RG=Reminder Grouping, SN=Serial Numbering

PA=Parity Assignment, RC=Row & Column

BC=Block Ciphering

TABLE II

2D Mapping Array M=3

	2	1	0
2	अ	आ	इ
1	ई	ट	प
0	இ	அ	ஆ

TABLE III

MTDAS DECRYPTION

BC	आ	ई	ट	அ	इ
RC	R,C	C,R	R,C	C,R	R,C
PA	ODD	EVEN	ODD	EVEN	ODD
SN	1	2	3	4	5
RG	2,1	2,1	2,2	1,0	2,0
R	2 1	2 1	2 2	1 0	2 0
Q	23 26	22 24	27 23	27 23	21 28
M	3	3	3	3	3
Unicode	71 79	68 73	83 71	82 69	65 84
Plaintext	G O	D I	S G	R E	A T

III.PROPOSED METHOD

A.EETUM

In this EETUM technique we use ENGLISH language, Numerals and combinations of both. Though many languages are being used in MTDAS if two people of different countries want to communicate they have to be aware of both of their native languages. But in EETUM only English is used as a plaintext where English is international languages which many people know so their communication becomes easy. From the substitution table S1 the plaintext English character is replaced by Multilanguage characters. Each specified Multilanguage character has an individual value in S1 table. In this the values for the Multilanguage character ranges from 20 to 63 and for numerals the values are assigned to be from 10 to 19 from S2 table in quotient value. Then the mapping value (M) is assigned serially from 1 to M. Then this M values are shifted right for next serial term and it continues up to last plaintext character. The assigned values are then divided by serial M values which give Quotient (Q), and reminder (R) value. The reminder values and quotient values are grouped by M. Then from substitution table S2 the grouped values are replaced by reminder assignment character and quotient assignment character. Now the two digit Q value is splitted into two parts. From the substitution table S2 the first part of Q is replaced by the quotient assignment character similarly the second part is also replaced and it continues. Then assign the serial numbers for grouped characters. If the serial number is odd then consider grouping R, Q otherwise consider grouping Q, R. The outcome is the encrypted plaintext.

B. Algorithm for EETUM Encryption

Input : Plaintext
Output : Block Cipher

Steps — Explanation

1. Get an input English plaintext character.
2. Assign a Multilanguage character using an S1 table.
3. Assign the equivalent random values for each character from S1 table.
4. Now assign the mapping value from 1 to M and right shift that M value for next serial term and so on.
5. Then divide the random values from mapping value M. We get quotient Q, and reminder R.
6. Group the Q values according to the M value.
7. Now separate the first two digit Q value into two parts and assign the quotient assignment character for each part from S2 table and so on for next terms.
8. Group the reminder values depending on M value.
9. Assign the reminder assignment character for grouped values from S2 table.
10. Assign the serial number for assigned characters.

11. If the serial number is odd then group the characters of R, Q else if it is even then group the characters of Q,R.

S1 TABLE – SUBSTITUTION TABLE IV

ENGLISH CHARACTERS	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
SUBSTUTATION TABLE	अ	ଏ	પ	૨	ଋ	உ	ೞ	ಐ	∩	ट	૮	୨	ঝ	ଓ	ல	મ	ઙ	ග	ઠ	ଡ	ഖ	૪	३	ਏ	ণ	ഥ
RANDOM VALUES(20-63)	60	42	38	24	63	59	47	33	21	62	54	46	32	28	20	51	49	61	23	34	52	48	30	22	31	55

S2 TABLE - SUBSTITUTION TABLE V

QUOTIENT VALUES	REMINDER VALUES			QUOTIENT CHARACTER ASSIGNMENT										REMINDER CHARACTER ASSIGNMENT									
padding value=0	0	0	0	Ը	Ψ	ʋ	ቶ	ङ	Ч	ぐ	一	Հ	È	Շ	ĭ	ו	း	ဘ	ะ	ච	ســ	₠	⁀
[19]0	0	0	1	Ղ	ɼ	ሐ	ሊ	ㄙ	¦	ち	二	Յ	Ë	ሁ	ΰ	װ	င	ဢ	ฑ	ධ	ج	₰	‡
[18]1	0	0	2	Ֆ	И	ш	ઢ	ɿ	く	げ	三	Ꮁ	Ӣ	Ն	ว	ב	൭	ၛ	แ	ඵ	ع	₡	⁑
[17]2	0	1	0	Ꭷ	Љ	ሰ	ቆ	ર	ヌ	ひ	上	Ի	Ӳ	რ	ന	ײ	ກ	ց	ข	ශ	ﺑ	₲	•
[16]3	0	1	1	Ձ	ɷ	ቀ	Ơ	ㅈ	ㄓ	つ	中	Գ	Ѓ	ト	Щ	ע	ຍ	ω	ร	ಚ	ﻫ	₢	‣
[15]4	0	1	2	ꞕ	Њ	ቻ	ቧ	ঝ	ㄣ	い	甲	Դ	ς	ხ	β	ף	ʃ	ၒ	ฒ	ක	ڠ	₣	″
[14]5	0	2	0	Ʊ	ѧ	ռ	ፍ	ঌ	ㄕ	う	下	Ք	ë	ტ	ϒ	פ	ၽ	၅	ค	ಲೀ	ـى	₳	-
[13]6	0	2	1	ա	Ә	ተ	Ɪ	৬	ㄆ	て	人	Ջ	Є	Ↄ	Σ	צ	ʔ	ɂ	า	ද	ح	£	‴
[12]7	0	2	2	ձ	Ч	ኀ	ᎃ	ಹ	ㄇ	じ	天	Ա	Ѥ	ʓ	δ	ק	ɕ	Ϛ	โ	ඛ	ﯙ	₥	⁄
[11]8	1	0	0	Շ	ǯ	ነ	Ɛ	ঽ	ㄘ	べ	丙	Ձ	ц	ღ	ϕ	ט	ഭ	ဣ	๔	හ	ڤ	₦	—
[10]9	1	0	1	ᵽ	п	ሆ	ዖ	ৡ	尢	す	地	Ч	Ӵ	Ω	э	ר	ʅ	ၜ	ๆ	ට	ﻏ	₴	⁅
	1	0	2											ϑ	Þ	ש	ൺ	ၤ	ฆ	ම	ﻍ	₩	⁆
	1	1	0											ጉ	θ	ת	ე	☆	ง	ඨ	ﺭ	₪	‖
	1	1	1											ᄀ	Ψ	מ	ඩ	ნ	๗	ර	ز	€	‷
	1	1	2											ქ	þ	❖	ຖ	ၛ	๕	ඉ	كر	₭	⁇
	1	2	0											ლ	Θ	ܐ	ທ	ၯ	๘	ග	ﺷﻮ	₮	⁗
	1	2	1											Ո	Ω	ㄥ	ງ	၉	จ	ಡ	ﺑﻮ	₵	⁉
	1	2	2											ቁ	ω	ـ	ຈ	ဘ	ฉ	ಜ	ﺮ	₱	‹
	2	0	0											Ⴍ	Ç	ܒ	ກ	ບ	ศ	ල	ﮋ	₫	⁈
	2	0	1											Ⴗ	Ⲭ	ᐟ	ஜ	ၓ	๖	ද	ر	א	›
	2	0	2											ლ	Μ	ൟ	ດ	ၔ	น	ඹ	ﮨ	נ	‼
	2	1	0											Ӡ	б	ﺪ	ໝ	၆	ย	ළ	ﺮ	ס	‿
	2	1	1											ჹ	ↄ	ﻪ	ໝ	ຟ	๕	ඔ	ﻻ	ג	ˋ
	2	1	2											ც	ϼ	ه	ອ	သ	ฯ	ඬ	ڨ	ח	†
	2	2	0											ჰ	ϖ	ے	ຢ	ဂ	ห	ථ	و	כ	‶
	2	2	1											ო	ζ	ﺴ	ꩻ	ၜ	พ	උ	ﻐ	ם	·
	2	2	2											ჭ	ϭ	ﻂ	ഉ	ຝ	ဏ	ඊ	ﺳﻮ	ן	ʹ

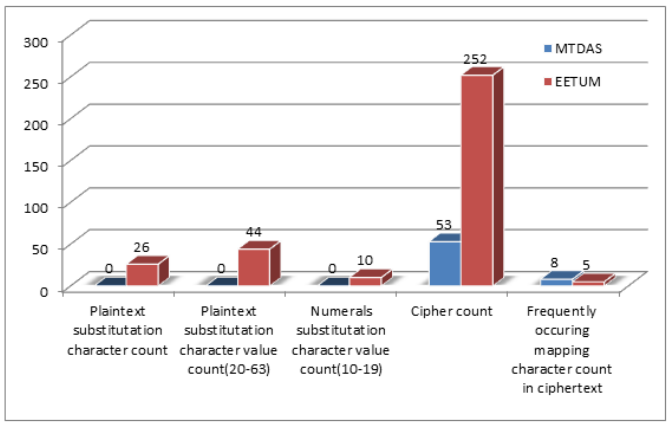
EETUM ENCRYPTION TABLE VI

Plain Text	I	N	D	I	A	1	2	3	-
Multilanguage Character	∩	ഖ	ટ	∩	अ	Ֆ	Ꮹ	Ω	
Assigned Value (A)	21	28	24	21	60	18	17	16	0
Mapping Value (M=3)	1	2	3	2	3	1	3	1	2
Quotient Q=A/M	21	14	08	10	20	18	05	16	00
Quotient Grouping		21,14,08			10,20,18			05,16,00	
Quotient Assigned Character		ᏫՖИᏠᏁᏤ			ᏯᎱᏝᏥᏜᎽ			ᏁᏅᎸᏭᏞΨ	
Reminder R=A mod M	0	0	0	1	0	0	2	0	0
Reminder Grouping		0,0,0			1,0,0			2,0,0	
Reminder Assigned Character		Ꮳ			Ꮽ			Ꮷ	
Serial Numbering		1			2			3	
Reminder (R) And Quotient (Q)		R,Q			Q,R			R,Q	
Block Ciphering		ᏣᏫՖИᏠᏁᏤ			ᏯᎱᏝᏥᏜᎽᏍ			ᏧᏁᏅᎸᏭᏞΨ	

EETUM DECRYPTION TABLE VII

Block Ciphering		ᏣᏫՖИᏠᏁᏤ			ᏯᎱᏝᏥᏜᎽᏍ			ᏧᏁᏅᎸᏭᏞΨ	
Reminder (R) And Quotient (Q)		R,Q			Q,R			R,Q	
Serial Numbering		1			2			3	
Reminder Assigned Character		Ꮳ			Ꮽ			Ꮷ	
Reminder Grouping		0,0,0			1,0,0			2,0,0	
Reminder R=A mod M	0	0	0	1	0	0	2	0	0
Quotient Assigned Character		ᏫՖИᏠᏁᏤ			ᏯᎱᏝᏥᏜᎽ			ᏁᏅᎸᏭᏞΨ	
Quotient Grouping		21,14,08			10,20,18			05,16,00	
Quotient Q=A/M	21	14	08	10	20	18	05	16	00
Mapping Value (M=3)	1	2	3	2	3	1	3	1	2
Assigned Value (A)	21	28	24	21	60	18	17	16	0
Multilanguage Character	∩	ഖ	ટ	∩	अ	Ֆ	Ꮹ	Ω	
Plain Text	I	N	D	I	A	1	2	3	-

IV. ANALYSIS OF MTDAS VS EETUM



(Plaintext = 106 Characters)
Fig.1 MTDAS VS EETUM

As an analysis the graph reveals the result, that there is no substitution for plaintext is used in MTDAS whereas in EETUM each 26 character are substituted by Multilanguage characters. Considering the plaintext of 106 characters with mapping constant M=3 the ciphertext count value for MTDAS is 53 so the count of the maximum repeating character in ciphertext is 8 times and the 3*3=9 mapping characters are coming atleast for 3 times and for EETUM the cipher count value is 252 due to this there is less number of characters get repeating and many more characters in S2 table does not appear in ciphertext so there is no relation between 'M' value and ciphertext. But in MTDAS the repeating 9 characters give the chance of getting M=3, so mapping value (M) prediction will be easy in MTDAS and it is quite difficult in EETUM.

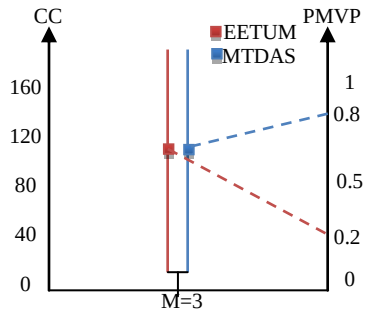


Fig.2 Frequency Analysis

CC=Character Count, M=Mapping value, PMVP=Probability of Mapping Value Prediction

As a frequency analysis reveals that in MTDAS if characters are increased in plaintext then mapping value is also to be increased or else the characters repetition in ciphertext will be more so probability of mapping value prediction ranges to high. Whereas in EETUM if number of characters in plaintext is increased there is no need to increase 'M' value, we can keep it constant. Since in EETUM there is no relation between 'M' value and frequently repeated ciphertext character count. Thus the probability of mapping value prediction in EETUM is low.

V. CONCLUSION AND FUTUREWORK

In this English Encryption Technique Using Multilanguage (EETUM) the ciphertext contain many Multilanguage characters. Thus it is difficult for frequency analysis and there is no need to send the quotient 'Q' value separately as done in MTDAS algorithm. In addition to characters, we can also use numerals in plaintext. In future we will consider about getting plaintext from Multilanguage as like English language.

VI. ACKNOWLEDGMENT

We thank Dr.U.Surya Rao, Principal & Dr.A.Kavitha Head of Department ECE, Chettinad College of Engineering & Technology for their kind support and help during the project completion.

REFERENCES

[1] G.Praveen Kumar et.al. "MULET: A Multilanguage Encryption Technique", Seventh International Conference on Information Technology, pp. 779-782, 2010.

[2] M.Rajendiran Et.al. "MTDAS: "Multilanguage block ciphering using two dimensional substitution array", Third International Conference, pp. 117 – 120, 2011.

[3] William Stallings - "Cryptography and Network security", fourth edition.

[4] Unicode Character form http://www.unicode.org

[5] C.Nelson Kennedy Babu Et.al. "Multilanguage Block Ciphering Using 3D Array", International Conference, ICECCS 2012, Kochi, India, August 9-11, 2012, pp. 255-261.

[6] Wikipedia.org/wiki/Visual_Cryptography.