Application of Advanced Cryptographic System

Meena Bairola[#1], Dr. A.S. Uniyal[*2]
[#]*Department of Mathematics*
M.B. (Govt.) P.G. College, Haldwani (UK), India

Abstract

In this paper we have defined some new definition of primes like Sam prime, Adherent prime, Extreme prime and Reverse prime and use them in cryptographic system for secure communication.

Keywords: *Sam prime, Adherent prime, Extreme prime, Reverse prime, Cryptography, Encryption, Decryption.*

INTRODUCTION

Cryptography was concerned with the conversion (encryption) of message from an understandable form into meaningless one and reverse again at the other end, rendering it unreadable by an unauthorized person without the information of secret key (decryption key). Cryptography is becoming a more essential topic in computer science. As there is a requirement for more secure cryptographic schemes, the application of number theory is going to increase for the developing secure encryption methods. S. Agarwal and A.S. Uniyal [1] have proposed a scheme for secure communication using prime weighted graph. Here in this paper we have designed an encryption algorithm using SAM prime and adherent primes.

NEW DEFINITONS

SAM PRIME: A prime number which is also a Mersenne, Fibonacci, Fermat as well as Lucas prime is called SAM prime. 3 is the only prime which is a SAM prime because it can be written as,

$M_2 = 2^2 - 1 = 3$ (Mersenne prime)

$u_4 = 1 + 2 = 3$ (Fibonacci prime)

$F_0 = 2^{2^0} + 1 = 3$ (Fermat prime)

$L_2 = L_0 + L_1 = 2+1 = 3$ (Lucas prime)

***ADHERENT PRIMES*:** Two or more primes are called adherent primes, if the sums of their digits are equal and also a prime.

Example: (i) 43 and 61 are adherent primes.

43 = 4+3 = 7

61= 6+ 1= 7

(ii) 137, 173, 191 are adherent primes.

137= 1+3+7= 11

173= 1+7+3 = 11

191= 1+9+1 = 11

(iii) 999727 and 999961 are adherent primes.

999727= 9+9+9+7+2+7= 43

999961= 9+9+9+9+6+1= 43

EXTREME PRIME: p = $d_0d_1d_2d_3d_4\ldots.d_n$ be a prime having more than three digits. By omitting all intermediate digits of prime p, we get a number $d_0\ d_n$, if this number $d_0\ d_n$ is a prime number then p is called an extreme prime. In other words, if the extreme digits of prime p also make a prime, then p is known as extreme prime.

Example: (i) 4447 is an extreme prime as its extreme digits 4 and 7 make a number 47, which is also a prime.
(ii) 999727 is an extreme prime as its extreme digits 9and 7 make a number 97, which is also a prime.

REVERSE PRIMES: p and q be the two different primes having m and n digits respectively. If the two numbers $p_{m,n}$ =pq and $p_{n,m}$ = qp are primes such that $p_{m,n} \neq p_{n,m}$ then $p_{m,n}$ and $p_{n,m}$ are called reverse primes.

Example: (i) $p_{2,1}$ = 113 and $p_{1,2}$ = 311 are reverse primes as 3 and 11 are two different primes such that 113≠ 311.
(ii) $p_{2,2}$ = 1319 and $p_{2,2}$ = 1913 are reverse primes as 13 and 19 are two different primes such that 1319 ≠ 1913.

CRYPTOGRAPHY

Cryptography [2] is the art and science of secure data communications over insecure channels. It is the study of technique of transferring messages in disguised form so that only the intended recipients can eliminate the disguise and interpret the message. Today, however, cryptography is everywhere! Security mechanisms that rely on cryptography are an integral part of almost any computer system.

CRYPTOGRAPHIC SYSTEM

A cryptographic system [3] is any computer system that involves cryptography. Such systems include for instance, a system for secure electronic mail which might include methods for digital signatures, cryptographic hash functions, key management techniques, and so on. Cryptographic systems are made up of cryptographic primitives [4], and are usually rather complex. Because of this, breaking a cryptosystem is not restricted to breaking the underlying cryptographic algorithms; usually it is far easier to break the system as a whole.

ENCRYPTION ALGORITHM

Password of Gmail: KAUSANI@26

Step I: Assign the ASCII value to each character of the message using Table 1.Table 2 shows the assignment of ASCII value to the characters.

Step II: Add the length of the string in ASCII value corresponding to each character. Here the length of the string is 10. The addition of the length of the string in the ASCII value is shown in table 3.

Step III: Assign a prime number for each numerical value getting after addition. If the value is a prime number then consider the number as it is and if the number is composite number then add/ subtract some value to it to make it a prime number just coming after/before it so that all the characters are to be assigned a prime number as shown in table 4.

Step IV: Now find adherent prime for each prime number just coming after it. Now make a key by using number of digits in each adherent prime as shown in table 5.

Step V: Add Sam prime to make another key as shown in table 6.

Table 1: ASCII value encryption chart

Decimal	Character	Decimal	Character	Decimal	Character	Decimal	Character
0	NUL (null)	32	SPACE	64	@	96	`
1	SOH (start of heading)	33	!	65	A	97	a
2	STX (start of text)	34	"	66	B	98	b
3	ETX (end of text)	35	#	67	C	99	c
4	EOT (end of transmission)	36	$	68	D	100	d
5	ENQ (enquiry)	37	%	69	E	101	e
6	ACK (acknowledge)	38	&	70	F	102	f
7	BEL (bell)	39	'	71	G	103	g
8	BS (backspace)	40	(	72	H	104	h
9	TAB (horizontal tab)	41	)	73	I	105	i
10	LF(NL line feed, new line)	42	*	74	J	106	j
11	VT (vertical tab)	43	+	75	K	107	k
12	FF(NP form feed, new page)	44	,	76	L	108	l
13	CR (carriage return)	45	-	77	M	109	m
14	SO (shift out)	46	.	78	N	110	n
15	SI (shift in)	47	/	79	O	111	o
16	DLE (data link escape)	48	0	80	P	112	p
17	DC1 (device control 1)	49	1	81	Q	113	q
18	DC2 (device control 2)	50	2	82	R	114	r
19	DC3 (device control 3)	51	3	83	S	115	s
20	DC4 (device control 4)	52	4	84	T	116	t
21	NAK (negative acknowledge)	53	5	85	U	117	u
22	SYN (synchronous idle)	54	6	86	V	118	v
23	ETB (end of trans. block)	55	7	87	W	119	w
24	CAN (cancel)	56	8	88	X	120	x
25	EM (end of medium)	57	9	89	Y	121	y
26	SUB (substitute)	58	:	90	Z	122	z
27	ESC (escape)	59	;	91	[	123	{
28	FS (file separator)	60	<	92	\	124	|
29	GS (group separator)	61	=	93	]	125	}
30	RS (record separator)	62	>	94	^	126	~
31	US (unit separator)	63	?	95	_	127	DEL

Table 2: Assignment of ASCII value to the character

Original message	**K**	**A**	**U**	**S**	**A**	**N**	**I**	**@**	**2**	**6**
ASCII value corresponding to each character	75	65	85	83	65	78	73	64	50	54

Table 3: Addition of the length of the string in the ASCII value

Original message	**K**	**A**	**U**	**S**	**A**	**N**	**I**	**@**	**2**	**6**
No. assigned to each character	75	65	85	83	65	78	73	64	50	54
Values after adding length of the string to ASCII value	85	75	95	93	75	88	83	74	60	64

Table 4: Assignment of a prime number to each character

Original message	**K**	**A**	**U**	**S**	**A**	**N**	**I**	**@**	**2**	**6**
Number assigned to each character	75	65	85	83	65	78	73	64	50	54
Values after adding length of the string to ASCII value	85	75	95	93	75	88	83	74	60	64
Value to be subtracted to make each no. of the string prime	2	2	6	4	2	5	0	1	1	3
Prime number corresponding to each character	83	73	89	89	73	83	83	73	59	61

Table 5: Assignment of an Adherent Prime to each prime number character

Original message	**K**	**A**	**U**	**S**	**A**	**N**	**I**	**@**	**2**	**6**
Number assigned to each character	75	65	85	83	65	78	73	64	50	54
Values after adding length of the string to ASCII value	85	75	95	93	75	88	83	74	60	64
Values to be subtracted to make each number of the string prime	2	2	6	4	2	5	0	1	1	3
Prime number corresponding to each character	83	73	89	89	73	83	83	73	59	61
Adherent prime corresponding to each prime no. character	137	73	179	179	73	137	137	73	59	151
Number of digits in each adherent prime no. character	3	2	3	3	2	3	3	2	2	3

Table 6: Assignment of SAM Prime to number of digits in each adherent prime number

Original message	**K**	**A**	**U**	**S**	**A**	**N**	**I**	**@**	**2**	**6**
Number assigned to each character	75	65	85	83	65	78	73	64	50	54
Values after adding length of the string to ASCII value	85	75	95	93	75	88	83	74	60	64
Values to be subtracted to make each number of the string prime	2	2	6	4	2	5	0	1	1	3
Prime number corresponding to each character	83	73	89	89	73	83	83	73	59	61
Adherent prime corresponding to each prime no. character	137	73	179	179	73	137	137	73	59	151
Number of digits in each adherent prime no. character	3	2	3	3	2	3	3	2	2	3
Adding SAM prime to the each digit	6	5	6	6	5	6	6	5	5	6

Table 7: First Decryption key

SAM prime number string	**6**	**5**	**6**	**6**	**5**	**6**	**6**	**5**	**5**	**6**

Table 8: String of other decryption key

String of decryption key to be subtracted	**3**	**3**	**3**	**3**	**3**	**3**	**3**	**3**	**3**	**3**
Resultant string of numbers	3	2	3	3	2	3	3	2	2	3

Now this string will give the information that how many digits we should consider to find the string of adherent primes as shown in table 9.

Table 9: String of prime number

Resultant string of numbers	**3**	**2**	**3**	**3**	**2**	**3**	**3**	**2**	**2**	**3**
Prime number	137	73	179	179	73	137	137	73	59	151

Find the Adherent prime for each prime number exist just before it except which are not adherent prime.

Table 10: Resultant string of Adherent Prime

Resultant string of Adherent primes	83	73	89	89	73	83	83	73	59	61

Table 11: Second decryption key

String of second Decryption key to be added	**2**	**2**	**6**	**4**	**2**	**5**	**0**	**1**	**1**	**3**
Resultant string of numbers	85	75	95	93	75	88	83	74	60	64

Table 12: String of number after adding length of string

Resultant string of numbers	**85**	**75**	**95**	**93**	**75**	**88**	**83**	**74**	**60**	**64**
Length of the string	10	10	10	10	10	10	10	10	10	10
Original string of number after subtraction	75	65	85	83	65	78	73	64	50	54

Table 13: Character corresponding to each number (ASCII VALUE) of the string

String of numbers	**75**	**65**	**85**	**83**	**65**	**78**	**73**	**64**	**50**	**54**
Corresponding character	K	A	U	S	A	N	I	@	2	6

Hence the original password is: **KAUSANI@26**

CONCLUSION

Cryptography is used to ensure that the contents of a message are confidentiality transmitted and would not be altered. The main aim of this paper was to propose and implement an algorithm so that data can be encrypted at client side before it is uploaded because it provides an extra layer of security and minimizes data theft in transit; therefore the proposed algorithm is useful for the security of passwords.

REFERENCES

[1] Shubham Agarwal, Anand Singh Uniyal, Prime Weighted Graph in Cryptographic System for Secure Communication, International Journal of Pure and Applied Mathematics (IJPAM), ISSN-1311-8080, Vol. No.105, No. 3, (2015), page: 325-338.

[2] Song Y. Yan, Computational Number Theory and Modern Cryptography, John Wiley & Sons, USA (2012).

[3] Shubham Agarwal, Anand Singh Uniyal, Elliptic Curves: An Efficient and Secure Encryption Scheme in Modern Cryptography, International Journal of Advance Research in Science and Engineering (IJARSE), ISSN-2319-8354, Vol. No.4, Issue 03, March (2015), page: 134-143.

[4] http://en.wikipedia.org/wiki/Cryptographic primitive.