"Science Stays True Here"
Journal of Mathematics and Statistical Science (ISSN 2411-2518, USA), Vol.6, Issue 11, 301-309 | Science Signpost Publishing

MMR Encryption Algorithm as an Alternative Encryption Algorithm to RSA Encryption Algorithm

Remzi Aktay

Kecioren Sehit Halil Isilar Middle School

Abstract

In this study, a public key encryption algorithm is tried to be developed. Unlike other public key encryption algorithms, it is desired to create a monitoring key next to the open and closed keys. While creating the algorithm, the equivalence of $a^{10^{n-1}}-b^{10^{n-1}} \equiv 0 \pmod{10^n}$ is used. Based on this equivalence, algorithms and keys have been created using modular arithmetic rules, Euclidean Algorithm, Euler Theorem, Euler Function, Factoring rules. The first difference of this algorithm from other algorithms is the observation key. In the event that private keys are stolen or cracked, hidden text or data cannot be accessed without a observation key. The second difference is that the receiver's private key, public key and observation key can take infinite values. For now, it is not a problem for the keys to take limited values in other algorithms. However, with the development and speed of the quantum computers, this will be a problem in the future. There are studies that have been successful in this regard. The third difference is that this algorithm has its own character code table. In addition, this algorithm is safer against side channel attacks.

Keywords: Encryption, Private Key, Monitoring Key, Euclid Algorithm, Euler's Theorem, Side Channel Attacks, Public Key Encryption

1. Introduction

Encryption algorithms can be listed as Transposition method, Substitution method, Symmetric Key Cipher method, Open Key Cipher method. These encryption methods were developed on the basis of security, respectively[1]. In symmetric key encryption, there is only one key, and the key of the message sender and the message receiver is the same and unique. This method is fast but insufficient in terms of security. There is a problem if the key is cracked or stolen. In the public key encryption method, the message receiver and sender have their own private key. Also encrypted text acts as a public key. The most

commonly used is the RSA Asymmetric Encryption Algorithm and the Elliptic Curve Encryption Algorithm. The RSA Encryption Algorithm is an algorithm based on the product of two very large prime numbers, and it is very difficult to decipher. However, the limited value of the private keys may be a problem in the future due to the increased computer speed. It is also open to timing analysis attacks, power analysis attacks, differential power analysis attacks, electromagnetic attacks, quantum computing power attack, acoustic crypto analysis attack and error analysis attacks, which are side channel attacks. Great progress has been made in this regard. Shamir and his team achieved successful results in 2013, especially in the Shor Algorithm, Acoustic crypto analysis attack on quantum computing power. Bellcore attack is known in 2010 for error analysis attack. In the algorithm developed in this study, first of all, private keys are prevented from taking limited values. The encrypted text cannot be accessed without using the observation key with the private key.

2. Method

Let a and b be two natural numbers whose last digits are the same.

$a-b\equiv 0 \pmod{10}$ x is the natural number greater than one.

Let's find the value of x that provides $a^x-b^x\equiv 0 \pmod{10^2}$

$a^x-b^x=(a-b).(a^{x-1}b^0 + a^{x-2}b^1 +\ldots.+ a^0b^{x-1}) \equiv 0 \pmod{10^2}$……(1)

$a\equiv b \pmod{10} \Rightarrow a^s\equiv b^s \pmod{10}$ “s” is a natural number …… (2)

If (2) is written in (1);

$a^x-b^x=(a-b).(a^{x-1}a^0 + a^{x-2}a^1 +\ldots..+ a^0a^{x-1})\equiv 0 \pmod{10^2}$

$a^x-b^x=(a-b).(a^{x-1} + a^{x-1} +\ldots..+ a^{x-1}))\equiv 0 \pmod{10^2}$

$a^x-b^x=(a-b).(x.a^{x-1})\equiv 0 \pmod{10^2}$…….(3)

The expression must always be at least x = 10 to be provided.

Let $a^{10}=m$ and $b^{10}=n$

y is a natural number greater than one;

Let's find the value y that provides $m^y-n^y\equiv 0 \pmod{10^3}$.

$m^y-n^y=(m-n).(m^{y-1}n^0 + m^{y-2}n^1 +\ldots.+ m^0n^{y-1}))\equiv 0 \pmod{10^{3\cdots}}$.(4)

If (2) is written in (4);

$m^y-n^y=(m-n).(m^{y-1}m^0 + m^{y-2}m^1 +\ldots.+ m^0m^{y-1}))\equiv 0 \pmod{10^3}$

$m^y-n^y=(m-n).(m^{y-1} + m^{y-1} +……..+ m^{y-1}))≡0 (mod10^3)$

$m^y-n^y=(m-n).(y.m^{y-1}))≡0 (mod10^3)$…… (5)

The expression must always be at least y = 10 to be provided.

$(a^{10})^{10}=m$ and $(b^{10})^{10}=n$ ……(6)

Let $a^{10^2}=p$, $b^{10^2}=q$

z is a natural number greater than one;

Let's find the value z that provides $p^z-q^z≡0 (mod\ 10^4)$.

$p^z-q^z=(p-q).(p^{z-1}q^0 + p^{z-2}q^1 +……+ p^0q^{z-1}))≡0 (mod10^4)$……(7)

If (2) is written in (7);

$p^z-q^z=(p-q).(p^{z-1}p^0 + p^{z-2}p^1 +……..+ p^0p^{z-1}))≡0 (mod10^4)$

$p^z-q^z=(p-q).(p^{z-1} + p^{z-1}+……..+ p^{z-1}))≡0 (mod10^4)$

$p^z-q^z=(p-q).(z.\ p^{z-1}))≡0 (mod10^4)$…….(8)

The expression must always be at least z = 10 to be provided.

It becomes $a^{10^3}- b^{10^3}≡0 (mod\ 10^4)$……(9)

If the same operations are done infinite times;

"n" is a natural number,

The equivalence $a^{10^{n-1}}- b^{10^{n-1}}≡0 (mod\ 10^n)$ is obtained……(10)

In the equation in (10), if 2 is written in the mode part, a and b numbers can be taken as twin prime numbers. This algorithm is created according to the equivalence established according to the twin prime numbers in (11).

$a^{2^{n-1}}- b^{2^{n-1}}≡0 (mod\ 2^n)$ a and b twin prime numbers …… .. (11)

3. Results

3.1. Generating Algorithm Keys

Based on the equivalence found in (11), the numbers “e” and “d” required for the private keys were created first. Euclidean algorithm and modular arithmetic rules were used in creating these numbers.

Let be an “e” number such that $1 ⟨ e ⟨ 2^n$. Such that;

Let $e.a≡1 (mod\ 2^n)$ ……(12)

Let's multiply each side of the equivalence in (11) by the number $e^{2^{n-1}}$.

$e^{2^{n-1}}$. $a^{2^{n-1}}$-$e^{2^{n-1}}$. $b^{2^{n-1}}$≡0 (mod 2^n)

If $(e.a)^{2^{n-1}}$-$(b.e)^{2^{n-1}}$ ≡0 (mod 2^n) is applied in (12);

$(b.e)^{2^{n-1}}$≡1 (mod 2^n)……..…..(13)

Let be an "d" number such that 1 ⟨d ⟨ 2^n. Such that;

Let d.b≡1 (mod 2^n) ……(14)

Let's multiply each side of the equivalence in (11) by the number $d^{2^{n-1}}$

$d^{2^{n-1}}$. $a^{2^{n-1}}$-$d^{2^{n-1}}$. $b^{2^{n-1}}$≡0 (mod 2^n)

If $(d.a)^{2^{n-1}}$-$(b.d)^{2^{n-1}}$ ≡0 (mod 2^n) is applied in (14);

$(a.d)^{2^{n-1}}$≡1 (mod 2^n)……..(15)

If (13) and (15) are combined;

$(a.b.e.d)^{2^{n-1}}$≡1 (mod 2^n)……(16)

If $(a.b.e.d)^{2^{n-1}}$≡1 (mod 2^n) is $(a.b.e.d)^{2^{n-1}}$=2^n.k+1, k is an integer.....(17)

Accordingly, the keys are formed as follows;

1-) The sender's private key is "a.b", in other words the twin prime numbers selected in the equivalence.

2-) The private key of the person receiving the message is "e.d", the numbers coming from (12), (14) and found by Euclidean Algorithm.

3-) Observation key $\mathbf{2^{n-1}}$

4-) The character of the character to be sent the public key is "m"; $\mathbf{m^{a.b}}$

3.2. MMR Character Code Table

KOD	CHAR	KOD	CHAR	KOD	CHAR	KOD	CHAR	KOD	CHAR	KOD	CHAR
1	(nul)	89	+	177	W	279	È	373	╣	445	▌
3	(soh)	91	,	179	X	281	Ô	375	║	447	▐
5	(stx)	93	-	181	Y	283	Ó	377	╗	449	▀
7	(etx)	95	.	183	Z	285	ı	379	╝	451	α
9	(eot)	97	/	185	[	287	ƒ	381	┘	453	β
11	(enq)	99	0	187	\	289	≈	383	┤	455	γ
13	(ack)	101	1	189	]	291	...	385	┐	457	π
15	(bel)	103	2	191	^	293	Ê	387	└	459	Σ
17	(bs)	105	3	193	_	295	Δ	389	┴	461	σ
19	(tab)	107	4	195	`	297	Ù	391	┬	463	μ
21	(lf)	109	5	197	a	299	ˆ	393	├	465	τ
23	(vt)	111	6	199	b	301	Ú	395	─	467	Φ
25	(np)	113	7	201	c	303	º	397	┼	469	θ
27	(cr)	115	8	203	d	305	˜	399	╞	471	Ω
29	(so)	117	9	205	e	307	0	401	╟	473	δ
31	(si)	119	:	207	f	309	Ö	403	╚	475	∞
33	(dle)	121	;	209	g	311	Ü	405	╔	477	Ø
35	(dc1)	123	<	211	h	313	-	407	╩	479	ε
37	(dc2)	125	=	213	i	315	£	409	╦	481	∩
39	(dc3)	127	>	215	j	317		411	╠	483	≡
41	(dc4)	129	?	217	k	319	Ş	413	═	485	±
43	(nak)	131	@	219	l	321	Ş	415	╬	487	≥
45	(syn)	133	A	221	m	323	.	417	╧	489	≤
47	(etb)	135	B	223	n	325	Ì	419	╨	491	⌠
49	(can)	137	C	225	o	327	Û	421	╤	493	⌡
51	(em)	139	D	227	p	329	·	423	╥	495	÷
53	(eof)	141	E	229	q	331	Ò	425	╙	497	≈
55	(esc)	143	F	231	r	333	□	427	╘	499	*o*
59	(fs)	145	G	233	s	335		429	╒	501	‘‘
61	(gs)	147	H	235	t	337	ğ	431	∏		-
63	(rs)	149	I	237	u	339	TL	433	╧	503	√
65	(us)	151	J	239	v	341		435	╪	505	∩
67	sp	153	K	241	w	343	‘‘	437	┘	507	²
69	!	155	L	243	x	345	Ω	439	┌	509	■
71	ì	157	M	245	y	347	º	441	▉	511	
73	#	159	N	247	z	349	0	443	▄		
75	$	161	O	249	{	351	´				
77	%	163	P	251		353	a				
79	&	165	Q	253	}	355	▒				
81	ë	167	R	255	~	357	▒				
83	(	169	S	257		359	▓				
85	)	171	T	259	Ç	361	┃				
87	*	173	U	261	ü	363	┤				
		175	V	263	È	365	╡				
				265	,	367	╢				
				267	‰	369	∏				
				269	‡	371	╕				
				271	Â						
				273	ç						
				275	Í						
				277	Î						

3.3. Working Principle of Algorithm

The algorithm works as follows.

First, each character of a text to be sent will be converted to MMR Character Codes. Let the code of a character in the text to be sent be the number "m".

1-) The person sending the message will encrypt this code with their own private key "a.b ".
The number "$m^{a.b}$ " is an encrypted number and will now serve as a public key.

2-) The recipient of the message will apply their private key to the incoming public key.
The number "$(m^{a.b})^{e.d} = m^{a.b.e.d}$" is still encrypted.

3-) The last observation key will be applied to the encrypted number.

It will be "$m^{(a.b.d.e)^{2^{n-1}}} \equiv x \pmod{2^n}$ ". If it is written in place of (17);

It becomes " $m^{(a.b.d.e)^{2^{n-1}}} = (m^{2^n})^k.m \equiv x \pmod{2^n}$ " …… (18)

Euler Function has $\theta(2^n)=2^{n-1}$ equation …… ..... (19)

"m" and "2" are coprime numbers
If $m^x \equiv 1 \pmod{2^n}$, x= $\theta(2^n)$ value provides this equivalence …… (20)
(18) in (19) and (20) are written in place;

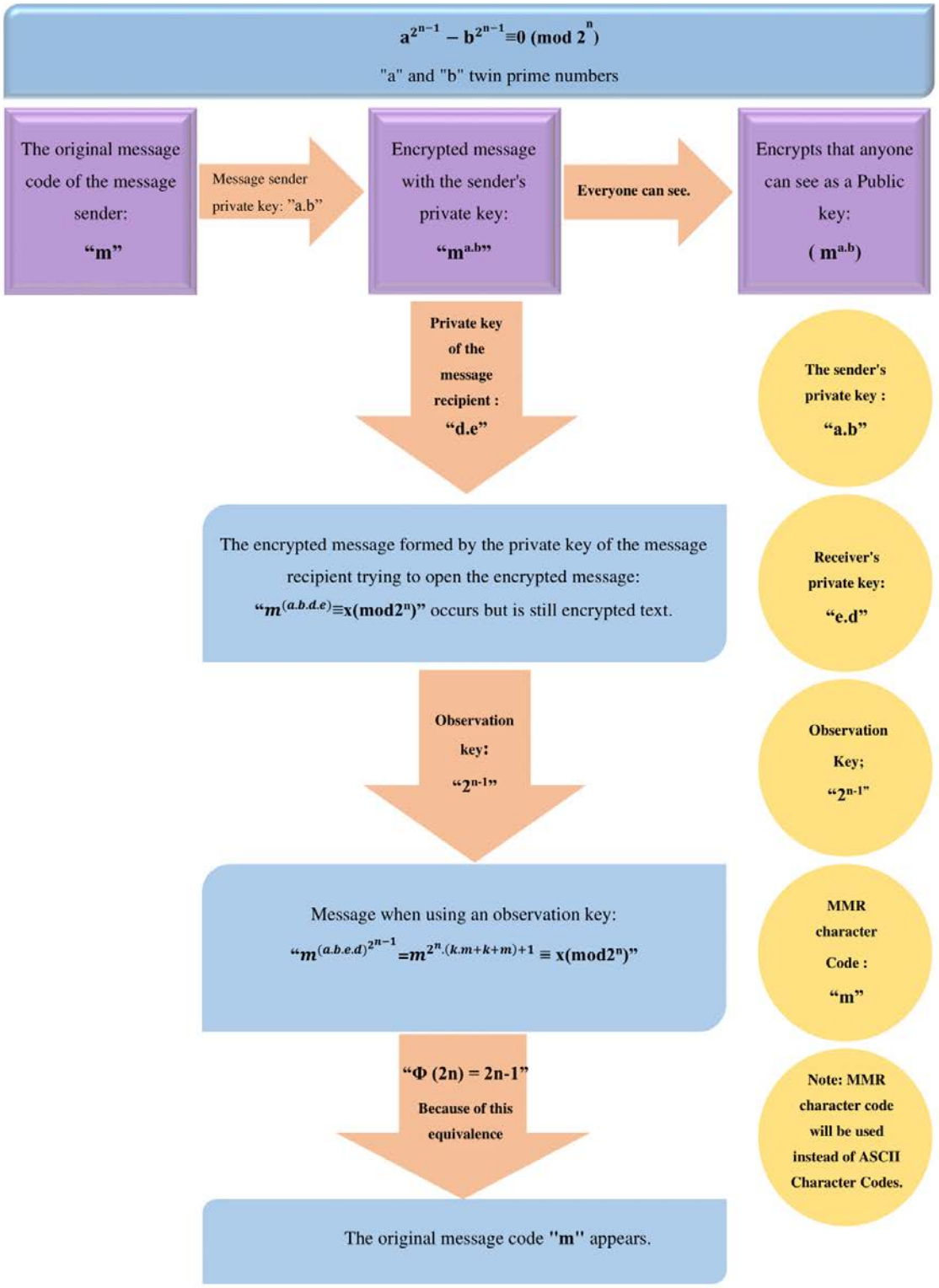
$m^{(a.b.d.e)^{2^{n-1}}} = (m^{2^n})^k.m \equiv x \pmod{2^n}$

$m^{(a.b.d.e)^{2^{n-1}}} = \left(m^{2^{n-1}}\right)^{2.k}.m \equiv x \pmod{2^n}$

From the expression $m^{(a.b.d.e)^{2^{n-1}}} = (1)^{2.k}.m \equiv x \pmod{2^n}$ comes the result of "x=m". (21)

As can be seen, the MRR Character Code of each character comes out of the algorithm as its own value. So the algorithm works.

3.3.1. Flow Chart



4. Conclusion and Discussion

When the equivalence in (11) is generalized, in any number base the force that makes the desired digit of the two digits on the same base the same as the last digit can always be found.

There are two reasons for using twin prime numbers in this algorithm. First, twin prime numbers can take infinite values just like prime numbers. Just as it is difficult to find prime numbers, it is very difficult to find twin prime numbers. The second reason is the number in the mod part is 2. The provision of the Euler Theorem in the algorithm depends on this. Because the Euler Function value of the 2^n number is 2^{n-1}, it must provide the Euler Theorem.

The reason for taking the equivalents used in selecting the numbers "e" and "d" as in (12) and (14); both to make it complex and to use the numbers "a" and "b" in the equivalence found at (11).

The private keys of the sender and the message recipient are taken as "a.b" and "e.d" because it gives the character code immediately in other crosses. For example; in case of receiving the closed key of the message "a.e", "a.d", "b.d", "b.e"; The public key actually becomes the desired character code because m^1 is the remainder. Taking the keys in this way occurred after many attempts.

In fact, it may seem like a disadvantage that the sender's private key is the product of the twin prime numbers and is constant. However, even if private keys are found, it does not make sense without an observation key. Also, the large numerical value of the key is a disadvantage for cracking it.

The reason for performing the operations and creating equivalencies in (13), (15), (17); is for the algorithm to provide. It makes it compulsory to use the observation key. In MMR Encryption Algorithm, the observation key and depending on the observation key, the fact that the sender's private key can get infinite value may cause it to work slowly for now. However, it is thought that when working with quantum computers in the future, it will be very important for the keys to get infinite value.

One of the attacks on the RSA Algorithm is the N Number Attack. As a result, N is the product of two prime numbers. This number can be easily reached with the development of computer technology. For this reason, it is easy to reach private keys easily. So MMR keys must take infinite value.

Acoustic Crypto Analysis Attack is an attack developed based on the sounds of the computer while it is operating. In private keys with limited value, studies were made to reach the values of these keys from the sounds in the study. Positive results have also been obtained. The infinite value of the keys ensures that this attack can also be prevented.

In short, positive results were obtained in the side channel attacks on the RSA Algorithm. MMR Encryption Algorithm is more advantageous in this regard. The fact that the algorithm depends on the twin

prime number and the long keys will provide many advantages in the future.

The reason for not using ASCII Character Codes in this algorithm is that Euler Theorem does not provide. For this reason, MMR Character Code table was created.

In this algorithm, keys may not be made by just changing the number "n". Keys can also be created by changing the twin prime numbers "a" and "b". However, the generated twin prime numbers may not always be easy. It would make more sense to change the software during the update.

References

[1]. Akben, B., Subaşı, A., "Comparison of RSA and Elliptic Curve Algorithm", Journal of Faculty of Science and Engineering, 2005, Kahramanmaraş, p. 36-40.

[2]. Invention, E., Yerlikaya, T. & Invention, N., "Key Exchange Systems in Asymmetric Encryption Algorithms", 2007, Kütahya: Dumlupınar University p. 1-2.

[3]. Akçam, N., "Error Correction and Digitally Signed Protocol Development Using RSA Algorithm", 2007, Ankara: Politeknik Magazine, p. 41-51.

[4]. Levi, A., Özcan, M., "Why is Public Key Based Encryption Difficult?", 2010 Istanbul: Sabancı University Faculty of Engineering and Natural Sciences p. 1-6.

[5]. Kodaz, H., Botsalı, F., "Comparison of Symmetric and Asymmetric Encryption Algorithms", 2010, Konya: Selçuk Technical Journal, p. 10-23.

[6]. Kartal, S. (2010). "Public Key Cryptography" https://www.savaskartal.com ›2010/04/13› open-keyed-cryptography

[7]. Beşkirli, A., Beşkirli, M., Özdemir, D., "An Investigation on Encryption Methods and RSA Algorithm", 2019, Istanbul: European Journal of Science and Technology. p. 284-291.

[8]. Hatun, E., "Side Channel Analysis on RSA Algorithm on Raspberry Pi", 2018, Istanbul Technical University Graduate Thesis, Institute of Science, p. 11-24.

[9]. Tarık Yerlikaya, Ercan Invention, H. Nusret Invention, "Cryptanalysis of RSA Encryption Algorithm Using Pollard RHO Method" Academic Informatics Conference, 31 January-2 February 2007, Trakya University Journal, Edirne 2007.