International Journal of Scientific Research in Computer Science and Engineering
Vol.8, Issue.6, pp.22-27, December (2020)

Research Paper

E-ISSN: 2320-7639

Hybrid of asymmetric cryptography (RSA) and symmetric cryptography (OTP)

Khean Ouk[1*], Kimsoung Lim[2], Sen samnang Ouk[3]

[1]Department of Computer Science, Royal University of Phnom Penh, Phnom Penh, Cambodia*[1]
[2]Department of IT, Emperor Bank PLC, Phnom Penh, Cambodia[2]
[3]Department of IT, Royal University of Phnom Penh, Phnom Penh, Cambodia[3]

**Corresponding Author*: *khean_ouk@yahoo.com.sg Tel: 855-12925849*

Available online at: www.isroset.org

Received: 20/Nov/2020, Accepted: 08/Dec/2020, Online: 31/Dec/2020

Abstract: Cryptography is a science-art that makes communication and messages more secure on the communication media, especially for state security, and business security and personal security. In the industrial revolution 4.0, security is a key to make communication more secure and the integrity and availability of data. The combination of symmetric cryptography and symmetric cryptography, symmetric cryptography and asymmetric cryptography, asymmetric cryptography and asymmetric cryptography is the main subjective to concern on security today. One of those combinations is a hybrid algorithm which is made up of asymmetric cryptography (RSA) and symmetric cryptography (OTP). It will strengthen the secureness of communication and data. This study will propose an Algorithm scheme to increase the security of cryptography. The result of the hybrid Algorithm shows steps to encrypt and decrypt the message: First of all, the sender encrypts the block of a message with the RSA public key and then generates the OTP key to encrypt this block of message again to obtain the double ciphertext from the same plaintext and then send it to the receiver. Finally, the receiver decrypts it with the OTP key and then the RSA private key. Therefore, we can say that the security of this proposed hybrid algorithm is more highly secured and guaranteed because of covering the weakness of the RSA cryptography. In conclusion, Section V describes the hybrid algorithm is highly secured and unbreakable.

Keywords: Cryptography, RSA, One Time Pad, Hybrid Algorithm, Symmetric Cryptography, Asymmetric Cryptography, Double cipher text.

I. INTRODUCTION

In the era of Technology challenge and IR4.0 that the world is connected as a village by using ICT to work from home, learn from home, and do business from home or anywhere as possible. There are some researchers who are trying to find a way to disrupt our services or steal our sensitive business data by breaking our security. There are some researchers who are trying to do research to find a way to strengthen our services or data as more and more secure as they can. Cryptography is an art of Science to manipulate the connection and message or data more secure into the form that can't be read or meaningless as it was captured between the source and the destination.

At this time, cryptography has become an object of research. It will be used to make the cryptography more secure by combining the two cryptographies together is the RSA and One Time Pad (OTP) to fill in the gap of each other. The result of this combination is called the hybrid algorithm of Cryptography. The result of the hybrid algorithm produces the two ciphertexts of a block of a message.

This paper will describe the sections are as follows: Section I describes the challenge of the RSA cryptography and the One Time Pad (OTP) cryptography and then reach to propose the hybrid algorithm, section II describes the layered architecture of the OSI model, TCP segment size, One Time Pad, RSA algorithm, Section III describes on how an RSA algorithm works, ASCII standard character set, encryption, decryption, section IV describes proposed algorithm schema and section V describes the secureness of the hybrid algorithm and its limitation and lack of ability to implement as an experimental.

II. RELATED WORK

When we are speaking about the Internet, everyone talks about TCP/IP protocol suite; this suit is not the only suit of protocols defined. It was established in 1947, the International Organization for Standardization (ISO) is a multinational body dedicated to the worldwide agreement on international standards. Almost three-fourths of the countries in the world are represented in the ISO. An ISO standard that covers all aspects of network communications is the Open System Interconnection (OSI) model. It was introduced in the late 1970s [1]. The OSI

model is a layered framework for the design of the network system. It consists of seven layers.

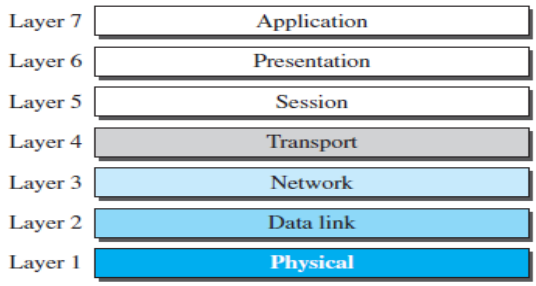

Fig. 1. The OSI model [1]

The transport layer is located between the application layer and the network layer of the TCP/IP protocol. It provides a process-to-process communication between two application layers, one at the local host and the other at the remote host. Communication is provided using a logical connection, which means that the two application layers, which can be located in different parts of the globe, assume that there is an imaginary direct connection through which they can send and receive messages. Figure 3.Shows the idea behind this logical connection [1].

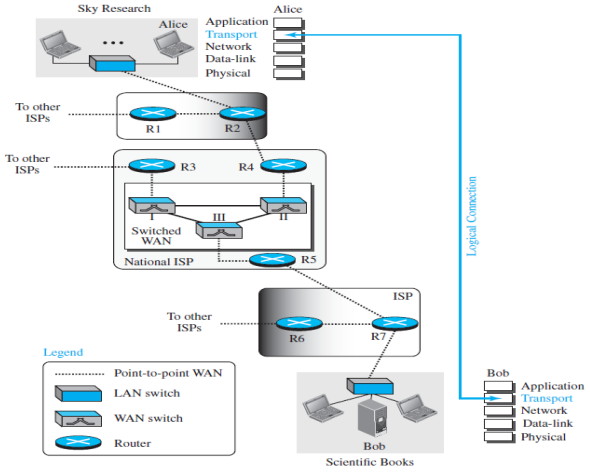

Fig. 2. Logical connection at transport layer [1]

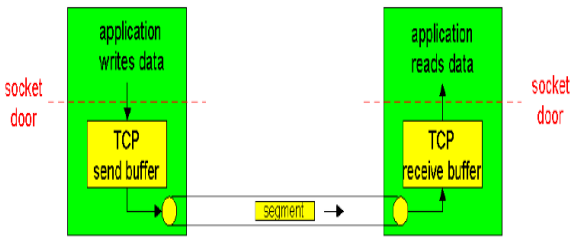

Fig. 3. TCP send and receive buffer [2]

The seven layer of the OSI model is divided into parts are upper layers which are application layer, presentation layer, and session layer. While other parts are the lower layer are the physical layer, the data link layer, and the network layer. The transport layer is a middle layer between the upper layer and the lower layer of the OSI model. The upper layer has a data size bigger than the lower layer size. That is a reason the message is broken into a piece of data. The data is at the upper layer of the OSI model is called Data or Message. To send a message from a sender to a receiver after establishing a session connection. The message will be broken into pieces in which each piece of data fits the size of the segment of the transport layer.

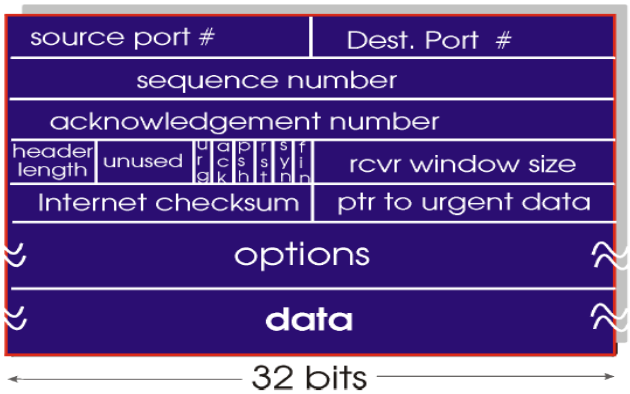

Fig. 4. TCP segment structure

The data is at the transport layer is called a segment. The default segment size is 536 bytes [2].

1. One Time Pad(OTP)

The One Time Pad is a stream cipher whose key is a random sequence of symbols from the alphabet. This algorithm is perfectly provided that the key generating process is completely random [3]. The encryption and decryption process of the One Time Pad (OTP) is using the XOR. The properties of the XOR returns the TRUE if and only if the value of both proposals is one of those are different. Otherwise, it will return the FALSE. It has a disadvantage as follows: If the length of the key and message are different. It will be vulnerable to the attacker or hackers. If the message is a very long steam of strings, it is very expensive to implement and take much time to do the operation. Once the key was used, it will not be used again. The key can't be in a textbook or notebook. If so, it will not be an OTP. If there will be only one path for transmission of the key, it may be an attacker intercepts that key and then it may be vulnerable to him. Even though the eve has the possibility to intercept it, but till now no way to attack (decrypt). The advantage of the OTP is that it cannot be broken for ciphertext.

2. RSA cryptography

Ron Rivest, Adi Shamir, and Len Adleman published RSA cryptography in 1978. RSA cryptography is asymmetric cryptography that uses two keys for the process. RSA cryptography is the most popular asymmetric cryptography that used because this algorithm has a benefit for key distribution. The process of generating the key for RSA cryptography mostly by the receiver. The receiver needs to generate both of the keys is a public key and a private key [3]. The RSA public key was known by everyone and the private key kept secret by the receiver or server.

III.METHODOLOGY

A. *Terminology:*

- *Plaintext:* This is the information to be protected during transmission.
- *Ciphertext:* The ciphertext is the denatured version of the plaintext produced by the encrypt algorithm that takes the plaintext and encryption key as input and generates cipher text.
- *Encryption:* The encryption is a process of doing the bitwise XOR operation between data stream and the secret key to make data message to be as ciphertext before transmitting
- *Decryption:* While decryption is a process of doing the bitwise XOR operation between a received data stream and a secret key to be as plaintext.
- *Double cipher text:* it is a plain text that was encrypted two times. The first one is with the public RSA key and the last one is with the OTP key.

B. *Algorithm*

1. Encryption and decryption with One Time Pad

○ *Encryption Process*

At the application layer of the OSI model, data are represented as ASCII code if this computer uses the ASCII code. If this computer uses the EDCDIC code, it is represented as the EDCDIC code.

$C_i = P_i \oplus K_i$ where C_i is Cipher Text, P_i is a block of plain text (TCP segment), K_i is a random key and it can be 1,2,3,….,n.

○ *Decryption process*

The receiver accepted the ciphertext from the lower layer and then does the decryption with the OTP key.

$P_i = C_i \oplus K_i$ where C_i is a cipher text, P_i is a block of plain text (TCP segment), K_i is a random key and it can be 1, 2, 3,…., n.

2. RSA algorithm

The RSA algorithm describes as the following:

- **Step1**: we generate two large prime number p and q and did not publish.
- **Step2**: we compute n where

$$n=pq \quad (1)$$

- **step3**: we Randomly select an integer e, where

$$\mathbf{(e,}\emptyset(n)) = 1 \quad (2)$$

- **Step4**:we compute an integer d, where

$$ed \equiv (mod, \emptyset(n)) \quad (3)$$

- it exists an integer d, thus e relatively prime with $\emptyset(n)$
- **Step5**: Publish n and e, but d must keep secret. If n is huge enough, even n and e were known. It is very hard to factor p and q. so the secret d cannot be derived

C. *The ASCII Character set(65-127)*

haracters 65 - 127

The second table, which contains characters 65 - 127, contains the standard Latin alphabet characters both lower and upper case, separated only by a few characters at 91 - 96 and 123 - 127.

Decimal	Octal	Hexadecimal	Character	Decimal	Octal	Hexadecimal	Character
065	101	41	A	097	141	61	a
066	102	42	B	098	142	62	b
067	103	43	C	099	143	63	c
068	104	44	D	100	144	64	d
069	105	45	E	101	145	65	e
070	106	46	F	102	146	66	f
071	107	47	G	103	147	67	g
072	110	48	H	104	150	68	h
073	111	49	I	105	151	69	i
074	112	4A	J	106	152	6A	j
075	113	4B	K	107	153	6B	k
076	114	4C	L	108	154	6C	l
077	115	4D	M	109	155	6D	m
078	116	4E	N	110	156	6E	n
079	117	4F	O	111	157	6F	o
080	120	50	P	112	160	70	p
081	121	51	Q	113	161	71	q
082	122	52	R	114	162	72	r
083	123	53	S	115	163	73	s
084	124	54	T	116	164	74	t
085	125	55	U	117	165	75	u
086	126	56	V	118	166	76	v
087	127	57	W	119	167	77	w
088	130	58	X	120	170	78	x
089	131	59	Y	121	171	79	y
090	132	5A	Z	122	172	7A	z

Fig. 5. ASCII Character Set

D. ASCII Character set(32-64)

Decimal	Octal	Hexadecimal	Character	Decimal	Octal	Hexadecimal	Character
032	040	20	Space	049	061	31	1
033	041	21	!	050	062	32	2
034	042	22	"	051	063	33	3
035	043	23	#	052	064	34	4
036	044	24	$	053	065	35	5
037	045	25	%	054	066	36	6
038	046	26	&	055	067	37	7
039	047	27	'	056	070	38	8
040	050	28	(	057	071	39	9
041	051	29	)	058	072	3A	:
042	052	2A	*	059	073	3B	;
043	053	2B	+	060	074	3C	<
044	054	2C	,	061	075	3D	=
045	055	2D	-	062	076	3E	>
046	056	2E	.	063	077	3F	?
047	057	2F	/	064	100	40	@
048	060	30	0				

Fig. 6. ASCII Character Set

IV. RESULT AND DISCUSSION

A. *Public-Key Cryptography*

Public-key cryptography is forms of cryptosystem in which encryption and decryption are performed using two different keys are a ***public key*** and a ***private key***. Those keys are mathematically related although knowledge of one key does not allow someone to easily determine the other key which meant that the public key was known by everyone and the private key is only the receiver known. As shown in Figure 7, the sender *A* uses the public key of receiver *B* (or some set of rules) to encrypt the plaintext message *M* which is a piece of a file to be sent and sends the ciphertext *C* to the receiver. The receiver applies its own private key (or rule set) to decrypt the cipher text *C* and recover the plaintext message *M*. Because pair of keys is required, this approach is also called ***asymmetric cryptography***. Asymmetric encryption can be used for ***confidentiality***, ***authentication***, or both. An application is used for public key cryptosystems [4].

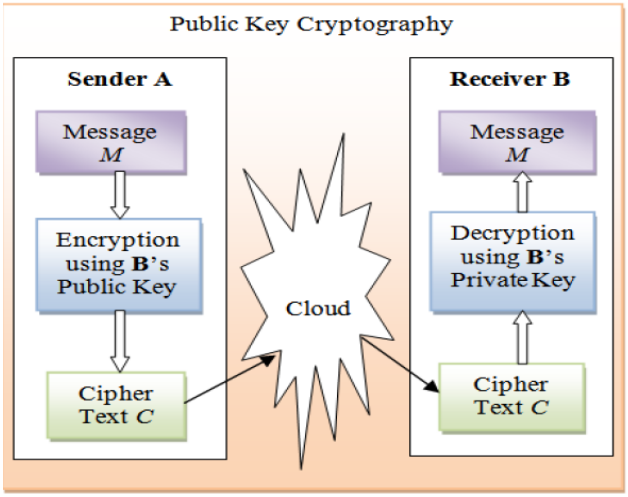

Fig.7. Public Key Cryptography [6]

The disadvantage of the RSA algorithm
It is vulnerable to brute force attacks, mathematical attacks, cryptanalysis attacks, and timing attacks. The first attack is through factoring modulus which results in the deciphering of messages, tractable [5].

B. *One Time Pad(OTP)*

Once the sender encrypts the message with the one-time pad (OTP), the sender destroyed the one-time pad. The receiver of the message uses the same one time pad to decrypt the ciphertext characters to plain text as an original one[6].

C. *Encryption Process*

The following is a process of converting the plain text to ASCII code and then binary code and last the hexadecimal base. The plain text is M (message): **hello** and a secret key were randomly generated as K (key):13579. From figure 4 and 5, we obtain the following:

Table.1. Plain text ASCII code

	P_1	P_2	P_3	P_4	P_5
Plain text	h	e	l	l	o
ASCII	104	101	108	108	111
Binary	01101000	01100101	01100100	01101100	01101111

Table.2. Key ASCII code

	K_1	K_2	K_3	K_4	K_5
Plain text	1	3	5	7	9
ASCII	49	51	53	55	57
Binary	00110001	00110011	00110101	00111101	00111001

The OTP encrypts each ASCII character by using the XOR with the key to obtain the ciphertext as follow:
$C_1=P_1 \oplus K_1 = 104 \oplus 49 = 59 =$;
$C_2=P_2 \oplus K_2 = 101 \oplus 51 = 56 = 8$
$C_3=P_3 \oplus K_3 = 108 \oplus 53 = 50 = 81 = Q$
$C_4=P_4 \oplus K_4 = 108 \oplus 55 = 50 = 2$
$C_5=P_5 \oplus K_5 = 111 \oplus 57 = 56 = 8$
So the cipher text is ;8Q28

D. *Decryption Process*

The OTP decrypts the ciphertext each ASCII code by using the key with XOR as follow:
$D_1=C_1 \oplus K_1 = 59 \oplus 49 = 104 = h$
$D_2=C_2 \oplus K_2 = 8 \oplus 51 = 101 = e$
$D_3=C_3 \oplus K_3 = 81 \oplus 53 = 108 = l$
$D_4=C_4 \oplus K_4 = 50 \oplus 55 = 108 = l$
$D_5=C_5 \oplus K_5 = 57 \oplus 56 = 111 = o$

E. *Proposed algorithm scheme*

To take advantage of the disadvantage of the RSA algorithm, we can implement the OTP on the ciphertext from the RSA public key encryption to obtain another ciphertext called **double cipher text**.

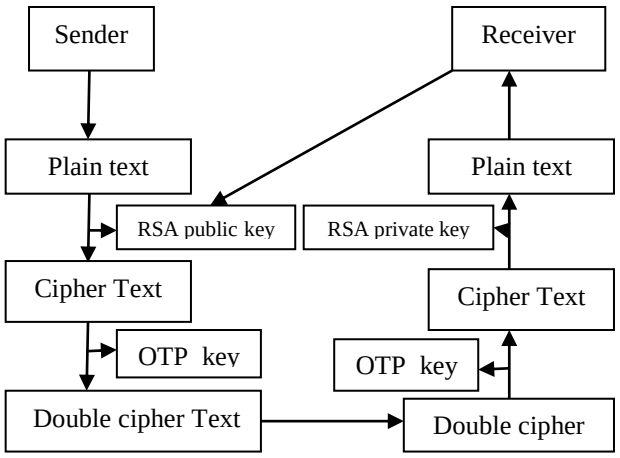

Fig.8. Proposed Algorithm scheme

E. implementation RSA and OTP with a python
- Encryption with RSA

- Encryption and Decryption with Python 3.The plaintext is “Angkor Wat is a World heritage belongs to the Kingdom of Cambodia”

Fig.9.Encrypt and decrypt a message with RSA

- Encryption and decryption with OTP

Fig.10.Encrypt the ciphertext with OTP again.

It is called a double ciphertext. The result of this program reveals that the string is 65 characters long and then it was encrypted by the RSA public key. The obtained ciphertext is 290 characters long. Finally, it was encrypted by the OTP. The number of keys is 26^290 equals to 1.989292945639 1465686215289925873e+87 keys. It is unbreakable. So it is strongly secure. The above key is one of them randomly selected.

V. CONCLUSION

As the result of the discussion on the advantage and disadvantage of asymmetric cryptography (RSA) and symmetric cryptography (OTP) and its implementation with current technology, it draws to conclude that use combination of the RSA algorithm and the OTP cryptography is exactly to increase the secureness of the cryptography called Hybrid Algorithm. Fig.9 and Fig.10 hybrid algorithm was implemented with python 3. For a network, we don’t implement yet. However, at the transport layer, the default TCP Maximum Segment Size is 536 bytes [8]. We can find out the number of ASCII code from this 536 bytes equals to 536 ASCII characters that will be encrypted with the OTP key. The length of these 536 bytes equals to 4288 bits longer than the RSA cryptography does. The RSA key can be 1024 bits or 2048 bits or 4096 bits. Today is a quantum computer that has high speed in transmission. So it doesn’t matter to encrypt and decrypt those bits.

The proposed hybrid algorithm is more secure compared to other hybrid algorithms and provides the capability of integrity of data and network connection because of double ciphertext was done by both RSA and OTP can fill in the gap of each other to make it more and more secure. Even though hacker can hack the RSA, but they cannot hack the OTP used to encrypt the data as the last step of encryption in Fig.10. As the result, it becomes more secure and can’t be vulnerable to any threats.

REFERENCES

[1]. Behrouz A. Forouzan, “*Data Communication and Networking”*, fifth edition, pp44-46, 2013.

[2]. James F. Kurose and Keith W. Ross, “Computer Networking: *A Top-Down Approach Featuring the Internet”*, pp 214-215, 2000.

[3]. M G Ristiana, R Marwati and S M Gozali, “*Hybrid algorithm of RSA and one time pad cryptography*”, 2019.

[4]. Shyam Nandan Kumar, “ *Review on Network Security and Cryptography”,* International Transaction of Electrical and Computer Engineers System, 2015, Vol. 3, No. 1, 1-11, 2015.

[5]. Nitin R. Mise, and H. C. Srinivasaiah, *“A Mathematical Attack Based Algorithm to Challenge the Security of RSA Cryptosystem”,* International Journal of Advancements in Research & Technology, Volume 2, Issue 6, June-2013 202 ISSN 2278-7763.

[6].Muhammad Iqbal, Muhammad Akbar Syahbana Pane,Andysah Putera Utama Siahaan, “*SMS EncryptionUsing One-Time Pad Cipher”* , IOSR Journal of Computer Engineering (IOSR-JCE),2016.

[7].Xiaoying Ye,Chenglian Liu, Donald Gardner3, “*Weakness of RSA Cryptosystem Characteristic*”, International Conference of Computational Methods in Sciences and Engineering 2018 (ICCMSE 2018).

[8]. Jon Postel,"Transmission Control Protocol," RFC 793,1981.

AUTHORS PROFILE

H.E.D.r. Khean Ouk graduated a Bachelor degree of Science in Mathematics in 1994 and Bachelor degree of Computer Science and Engineering in 2001 and master degree of Information Technology in 2006 from Royal University of Phnom Pen and Ph.D. in information technology in 2014, USA. He teaches Computer Networks, Computer Security and Linux System Administration and STEM education at the undergraduate level. His areas of research include Cryptography, STEM Education, and Computer Security, Computer Networks and Programming Languages. He has been working as IT lecturer since 1996 at Royal University of Phnom Penh and advisor to Ministry of Education Youth and Sport in Cambodia by his majesty of the King of Cambodia, his reputation and legacy. He has taught 20000 students at Bachelor Degree of Computer Science and Master of IT students. He published 10 papers with local journal at research department of Royal University of Phnom Penh and wrote and translated more than 20 IT books for teaching at Computer Science Department in Cambodia. Currently he is working as IT consultant to Baccalaureate Examination System in IT at Ministry of Education Youth and Sport in Cambodia, in charge of Digital Education and also work as Chairman of CaNOI(Cambodia National Olympiad in Informatics) and IOI (International Olympiad in Informatics). With the CaNOI/NOI and IOI, he has taught the algorithm and C++ programming for competition.

Mr. Kimsoung Lim graduated a Bachelor degree of Computer Science and Engineering in 2016 at Royal University of Phnom Penh. He works as a deputy IT Manager for M.G.N Emperor banking since 2018. His daily job is to control the system security and system network administration on Linux system and Windows server. His areas of research include vulnerability assessment of system and appliance firewall (F5) and machine learning on how a computer works for specific task for banking. He is pursuing a Master degree of IT Engineering at Royal University of Phnom Penh.

Mr. Sen Samnang Ouk graduated a Bachelor degree of Computer Science and Engineering in 2019 at Royal University of Phnom Penh. Currently he works as a system developer (modify, analyze, Design and implement of Enterprise Service Bus) for Amreth Microfinance since 2019. His areas of research include AI, Machine Learning and Security applications. He is pursuing a Master degree of Computer Science and Engineering at Royal University of Phnom Penh.

