MIS Review Vol. 19, No. 2, March (2014), pp. 1-13
DOI: 10.6131/MISR.2014.1902.01

Hybrid Encryption/Decryption Technique Using New Public Key and Symmetric Key Algorithm

Prakash Kuppuswamy[1], Saeed Q. Y. Al-Khalidi[2]
[1]*Department of Computer Engineering & Networks, Jazan University, KSA*
[2]*Deanship of Libraries Affairs, King Khalid University, KSA*

ABSTRACT: *This research study proposes Hybrid Encryption System using new public key algorithm and private key algorithm. A hybrid cryptosystem is one which combines the convenience of a public-key cryptosystem with the efficiency of a symmetric-key cryptosystem. Here, we propose a provably two way secured data encryption system, which addresses the concerns of user's privacy, authentication and accuracy. This system has two different encryption algorithms have been used both in the Encryption and decryption sequence. One is public key cryptography based on linear block cipher another one is private key cryptography based on simple symmetric algorithm. This cryptography algorithm provides more security as well as authentication comparing to other existing hybrid algorithm.*

KEYWORDS: *Asymmetric Key, Hybrid Encryption, Modular, Symmetric Key.*

1. Introduction

Hybrid encryption is a mode of encryption that merges two or more encryption systems. It incorporates a combination of asymmetric and symmetric encryption to benefit from the strengths of each form of encryption. These strengths are respectively defined as speed and security.

Hybrid encryption is considered a highly secure type of encryption as long as the public and private keys are fully secure. A hybrid encryption scheme is one that blends the convenience of an asymmetric encryption scheme with the effectiveness of a symmetric encryption scheme. Hybrid encryption is achieved through data transfer using unique session keys along with symmetrical encryption. Public key encryption is implemented for random symmetric key encryption. The recipient then uses the public key encryption method to decrypt the symmetric key. Once the symmetric key is recovered, it is then used to decrypt the message.

The combination of encryption methods has various advantages. One is that a connection channel is established between two users' sets of equipment. Users then have the ability to communicate through hybrid encryption. Asymmetric encryption can slow down the encryption process, but with the simultaneous use of symmetric encryption,

both forms of encryption are enhanced. The result is the added security of the transmittal process along with overall improved system performance (Janssen, n.d.).

The hybrid cryptosystem is itself a public-key system, who's public and private keys are the same as in the key encapsulation scheme. In place of public key system we can use digital signature like message digesting function with symmetric key system to make hybrid crypto system. Note that for very long messages the bulk of the work in encryption/ decryption is done by the more efficient symmetric-key scheme, while the inefficient public-key scheme is used only to encrypt/decrypt a short key value. For example, to encrypt a message addressed to user-1 in a hybrid technique user-2 does the following (Elminaam, Kader & Hadhoud, 2010; Gupta1 & Parvinder, 2013).

- Obtains user-1 public key.
- Generates a fresh symmetric key.
- Encrypts the message using the symmetric key.
- Encrypt the symmetric key using user-1 public key. And send both of these encryptions to user-1.

To decrypt this hybrid cipher text, user-1 does the following:

- User-1 uses her private key to decrypt the symmetric key.
- User-1 uses this symmetric key to decrypt the message.

Figure 1 shows the general diagram of Integration security between the various sources such as application software, hardware, user and resources etc.

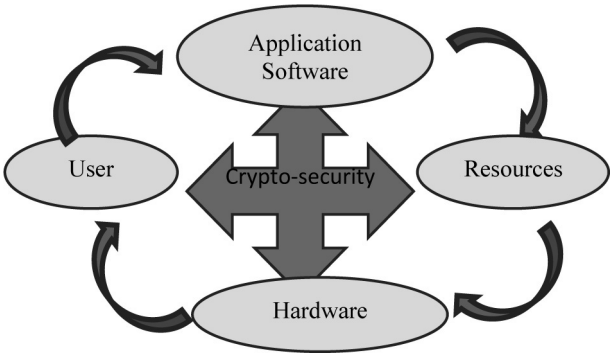

Figure 1 Integration of Data Security

2. Literature review

Shaar, Saeb, Elmessiery and Badawi (2003). In this proposal, encryption algorithm that can be used for hardware-implemented applications to secure data communications, this encryption algorithm is based on hiding a number of bits from plain text message into a random vector of bits. The name demonstrates the two basic operations of this algorithm, these operations include inserting part of the plaintext bits into a cover to hide it from recognition, that is, there are no conventional operations on the ciphered text, just plain hiding in a random bit string, the name hybrid is used to show that the algorithm has built-in features that are inherited from data hiding techniques or steganography.

Ramaraj, Karthikeyan and Hemalatha (2009), design the new security protocol using hybrid encryption technique for on line transaction. The hybrid encryption technique is a combination of both symmetric and asymmetric cryptographic techniques. It provides all the three cryptographic primitives -- integrity, confidentiality and authentication. In this proposed design methodology, the new protocol design using Symmetric cipher (AES-Rijndael) and public key cryptography (RSA) with hash function.

Tat Wi (2010) in this project, encryption will be implemented in information on a web that makes it hard to be readable and secure. In this encryption, it uses the substitution cipher in which each letter in the plaintext is replaced by some fixed number of position down the alphabet. This method is names after Julius Caesar who using this method to communicate with his generals. The result from this project is a data which is encrypted and be decrypted to its readable form. As a conclusion, Caesar cipher algorithm can be implemented in hybrid encryption project to make data secure and better.

Kuppuswamy and Chandrasekar's (2011) paper deals with a new algorithm, which is based on linear block cipher. The concept of this new algorithm is based on modular 37 (alphabets and numerals) whereas existing algorithms are based only on modular 26 (only alphabets). We are naming this linear based algorithm as New linear block cipher or Nlbc.

Kuppuswamy and Al-Khalidi (2012) proposed research main goal is to reflect the importance of security in network and provide the better encryption technique for currently implemented encryption techniques in simple and powerful method. In this research we have proposed a modular 37 and select any number and calculate inverse of the selected integer using modular 37. The symmetric key distribution should be done in the secured manner. Also, we examine the performance of our new SSK algorithm with other existing symmetric key algorithm.

3. Research objectives

Privacy is one of the key issues addressed by information Security. Through cryptographic encryption methods, one can prevent a third party from understanding transmitted raw data over unsecured channel during signal transmission. The cryptographic methods for enhancing the security of digital contents have gained high significance in the current era. Breach of security and misuse of confidential information that has been intercepted by unauthorized parties are key problems that information security tries to solve. This paper sets out to contribute to the general body of knowledge in the area of classical cryptography by developing a new hybrid way of encryption of plaintext.

DES algorithm is now considered insecure for many applications and has many weaknesses. This is mainly because its 56-bit key size is too small. Many attacks and methods that exploited the shortcomings of DES have rendered it an insecure block cipher. Triple DES which is an enhancement to DES was later proposed in which the original DES algorithm was applied thrice to increase the security. But it was found to be very slow. The most preferred algorithm is AES. It is considered to be the best encryption standard. Brute force attack is the only known possible attack against AES algorithm. Our proposed hybrid algorithm is found to be the best encryption standard and is given priority over other standards.

4. Proposed algorithm structure

The proposed algorithm architecture of encryption and decryption method mentioned in the Figure 2 and procedure of the algorithm were as follows:

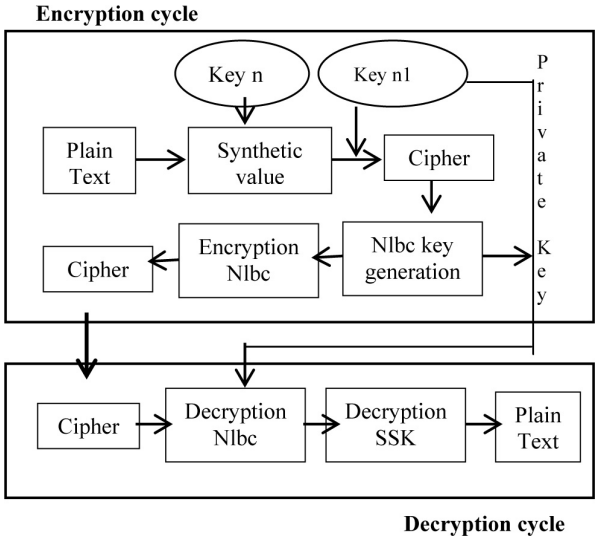

Figure 2 Encryption/Decryption Structure

4.1 Symmetric key algorithm (SSK)

4.1.1 SSK key generation method

(1) Select any natural number say as "n."

(2) Find the Inverse of the number using modulo 37 (key 1) say "k."

(3) Again select any negative number (for making secured key) "n1."

(4) Find the inverse of negative number using modulo 37 (key 2) "k1."

4.1.2 Encryption method

(1) Assign synthetic value for message.

(2) Multiply synthetic value with random selected natural number.

(3) Calculate with modulo 37.

(4) Again select random negative number and multiply with it.

(5) Again calculate with modulo 37 CT = (PT × n × n1) mod 1.

4.1.3 Decryption method

(1) Multiply received text with key 1 & key 2.

(2) Calculate with modulo 37.

(3) Remainder is Revealed Text or Plain Text PT = (CT × n–1 × n1–1) mod 1.

4.2 Linear block cipher algorithm

The algorithm of encryption and decryption of the technique is to use text and numbers during implementation of the message algorithm which is as follows.

Here, we introduce our Nlbc algorithm asymmetric or public key algorithm. The major advantage of asymmetric cryptography is to use two different keys, one Public (open) key and one Private (secret) key. The encrypted message by sender can be decrypted by the other at receiving end and vice versa.

4.2.1 Encryption technique

Step 1: To encrypt a text message at first the given text and numbers are stored in a string variable, say ***m***.

Step 2: Select $k \times k$ square matrix called as k.

Step 3: Select any integer value say as e.

Step 4: Make plain text or message as blocks according to the *k* matrix. And transpose the selected block.

Step 5: Multiply Plain text or message with selected square matrix and e value.

Step 6: Use modulation 37 with derived message. The remainder is Cipher text or decrypted message. Announce Cipher text, *e*, 37 as public key, and k as private key sent to the receiver in secured channel.

4.2.2 Decryption technique

Receiving the plaintext from cipher text using the key is called decryption or deciphering or decoding. Our New linear block cipher decryption sequences were as follows:

Step 1: Receiving Cipher text and Private key *k'* and *e'*.

Step 2: Arrange encrypted message as *r* blocks.

Step 3: Calculate with cipher text using Private key and d.

Step 4: Make modulo 37 with calculated message. The remainder value is called Plain Text.

Step 5: Now we use modulation with calculated value the remainder text is called our Plain Text.

5. Implementation

Encryption is the formal name for scrambling program. The normal data, unscrambled, called plaintext or clear text and transform them so that unintelligible to the outside observer, the transformed data is called enciphered text or cipher text. Using encryption security professional can virtually nullify the value of an interception and the possibilities of effective modification and fabrication. Encryption is clearly addressing the need for confidentially of data. Additionally, it can used to ensure integrity, that the data cannot be read generally cannot be easily changed in the meaningful manner. It is basis of the protocol that enables to provide security while accomplishing an important system or network task. A protocol is an agreed-on sequence of actions that leads to desirable results. For example, some operating system protocols ensure availability of resources as different tasks and users request them. Thus, encryption can also be thought of as supporting availability. That is, encryption is at the heart of methods for ensuring all aspects of computer security. For the implementation of the proposed algorithm, we have selected sample data "NETWORK DEPARTMENT 2014." The synthetic value assigned for the sample data mentioned in Table 1.

Table 1 Sythetic Value of Alphabets

N	**E**	**T**	**W**	**O**	**R**	**K**
14	5	20	23	15	18	11
D	**E**	**P**	**A**	**R**	**T**	**M**
4	5	16	1	18	20	13
E	**N**	**T**	**2**	**0**	**1**	**4**
5	14	20	29	27	28	31

A. Key generation

(1) We are selecting random integer number n = 3.

(2) Then inverse of 3 = 25 (verification $3 \times 25 \bmod 37 = 1$). So, key 1 = 25.

(3) Again we are selecting random negative number n1 = -8.

(4) Then inverse of -8 = 23 (verify $-8 \times 23 = -184 \bmod 37 = 1$). So, key 2 = 23.

B. Encryption using SSK

The first phase of symmetric key algorithm using by SSK shown in the Table 2.

C. Encryption using Nlbc public key algorithm

$$= \begin{pmatrix} 1 & 2 & 1 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} \times \begin{pmatrix} 34 \\ 28 \\ 1 \end{pmatrix} \times 5 \bmod 37 = \begin{pmatrix} 11 \\ 4 \\ 24 \end{pmatrix}$$

Similarly encryption other text using key matrix, then we will get 11, 4, 24, 27, 4, 9, 6, 5, 20, 9, 35, 15, 22, 16, 26, 30, 27, 28, 10, 16, 25 i.e., encrypted message is "KDX0DIFETI8OVPZ301JPY" as mentioned in the following Table 3.

D. Decryption method using Nlbc public key

$$= \begin{pmatrix} 18 & 23 & 32 \\ 1 & 25 & 12 \\ 18 & 1 & 18 \end{pmatrix} \times \begin{pmatrix} 11 \\ 4 \\ 24 \end{pmatrix} 15 = \begin{pmatrix} 34 \\ 28 \\ 1 \end{pmatrix}$$

After 1 cycle Decryption the value of cipher text is 34, 28, 1, 3, 10, 12, 32, 15, 28, 23, 13, 12, 1, 21, 28, 34, 1, 7, 18, 31, 33 i.e., the equivalent value of Networking Department 2014 cipher message is "71ACJL5O1WMLAU17AGR46" as mentioned in the following Table 4.

E. Decryption using SSK private key

The final phase of the decryption algorithm using by the SSK shown in the Table 5.

Table 2 Symmetric Encryption

Plain Text	Integer Value	CT = (M × n) mod 37	CT = (CT × n1) mod 37	Cipher Text
N	14	5	34	7
E	5	15	28	1
T	20	23	1	A
W	23	32	3	C
O	15	8	10	J
R	18	17	12	L
K	11	33	32	5
D	4	12	15	O
E	5	15	28	1
P	16	11	23	W
A	1	3	13	M
R	18	17	12	L
T	20	23	1	A
M	13	2	21	U
E	5	15	28	1
N	14	5	34	7
T	20	23	1	A
2	29	13	7	G
0	27	7	18	R
1	28	10	31	4
4	31	19	33	6

Table 3 Asymmetric Encryption

	Encrypted Value	Alphabet Value
Block 1	11, 4, 24	K, D, X
Block 2	27, 4, 9	0, D, I
Block 3	6, 5, 20	F, E, T
Block 4	9, 35, 15	I, 8, O
Block 5	22, 16, 26	V, P, Z
Block 6	30, 27, 28	3, 0, 1
Block 7	10, 16, 25	J, P, Y

Table 4 Asymmetric Decryption

	Decrypted Value	Alphabet Value
Block 1	34, 28, 1	7, 1, A
Block 2	3, 10, 12	C, J, L
Block 3	32, 15, 28	5, O, 1
Block 4	23, 13, 12	W, M, L
Block 5	1, 21, 28	A, U, 1,
Block 6	34, 1, 7	7, A, G
Block 7	18, 31, 33	R, 4, 6

Table 5 Symmetric Decryption Process

Cipher Text	PT = (CT × 23 × 25) mod 37	Cipher Text
34	14	N
28	5	E
1	20	T
3	23	W
10	15	O
12	18	R
32	11	K
15	4	D
28	5	E
23	16	P
13	1	A
12	18	R
1	20	T
21	13	M
28	5	E
34	14	N
1	20	T
7	29	2
18	27	0
31	28	1
33	31	4

6. Result & discussion

The encryption/decryption algorithm is compared on the basis of time consumption check which pair of algorithms is more efficient for hybrid encryption/decryption of messages. We have taken various different message lengths are used and results are drawn as shown in the following Table 6. Figure 3 shows results of time consumed by the various pairs of algorithm in graphical form. It illustrates the execution time in milliseconds taken by each pair of algorithms to hybrid encrypt/decrypt the message of various different sizes mentioned in Table 7 and Figure 4. The graph shows that the combination of linear block cipher -- Symmetric key takes minimum time so it executes faster than RSA-DES and RSA-AES. The overall performance evaluation of RSA-DES, RSA-AES and new proposed algorithm mentioned in Figure 5.

Table 6 Key Generation Timing of Algorithm

Algorithm	Key Generation Time
RSA-DES	6 Sec
3 DES	12 Sec
RSA-AES	8 Sec
Proposed Algorithm	4 Sec

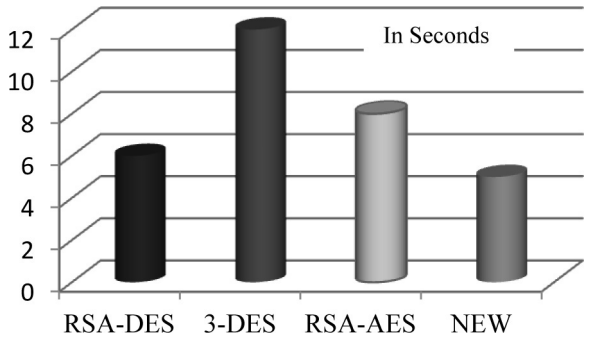

Figure 3 Key Generation Timing

Table 7 Comparison of Data Execution Time

No. of Bits	RSA 3DES	RSA-AES	Proposed Algorithm
100	220 ms	245 ms	210 ms
300	280 ms	295 ms	260 ms
500	310 ms	320 ms	290 ms
1,000	390 ms	400 ms	350 ms

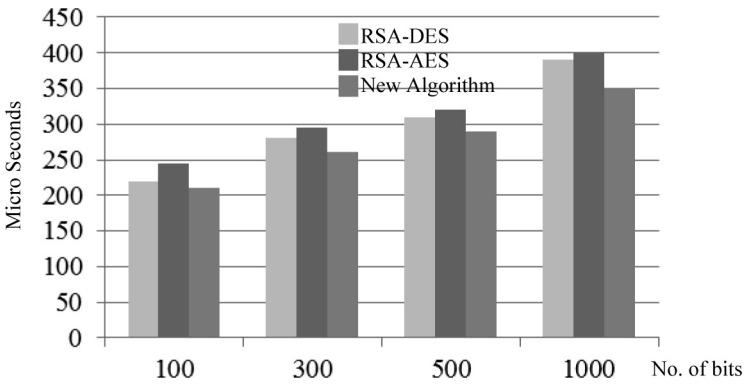

Figure 4 Encryption Executing Timing

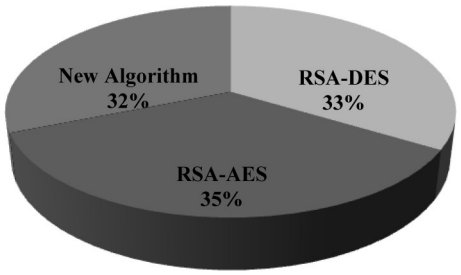

Figure 5 Performance of Algorithm

7. Conclusion

The encryption and decryption of any data has a secure key, which is used for data encryption. For this purpose asymmetric key is used. This work secures the data, using linear block cipher algorithm. The block cipher algorithm is more efficiently using in symmetric encryption technic. The result of the proposed research plan shows that processing time is more efficient other algorithm. Thus AES algorithm along with the use of RSA algorithm for key management will provide an efficient technique to ensure the security of transmitted data. The security RSA AES better than RSA-DES and our proposed algorithm is efficient than RSA AES during the application of data transmission. Finally we illustrated the new directions for the future research. We can develop the derivatives of outburst attack. Thus the proposed Hybrid Encryption Algorithm using Block cipher and symmetric key provides a more secure and convenient technique for secure data trans-mission for all kind application.

References

Elminaam, D.S.A., Kader, H.M.A. and Hadhoud, M.M. (2010), 'Evaluating the performance of symmetric encryption algorithms', *International Journal of Network Security*, Vol. 10, No. 3, pp. 213-219.

Gupta1, R.K. and Parvinder, S. (2013), 'A new way to design and implementation of hybrid crypto system for security of the information in public network', *International Journal of Emerging Technology and Advanced Engineering*, Vol. 3, No. 8, pp. 108-115.

Janssen, C. (n.d.), 'Hybrid encryption', available at http://www.techopedia.com/definition/1779/hybrid-encryption (accessed 22 November 2014).

Kuppuswamy, P. and Al-Khalidi, S.Q.Y. (2012), 'Implementation of Security through simple symmetric key algorithm based on modulo 37', *International Journal of Computers & Technology*, Vol. 3, No. 2, pp. 335-338.

Kuppuswamy, P. and Chandrasekar, C. (2011), 'Enrichment of security through cryptographic public key algorithm based on block cipher', *Indian Journal of Computer Science and Engineering*, Vol. 2, No. 3, pp. 347-355.

Ramaraj, E., Karthikeyan, S. and Hemalatha, M. (2009), 'A design of security protocol using hybrid encryption technique', *International Journal of the Computer, the Internet and Management*, Vol. 17, No. 1, pp. 78-86.

Shaar, M., Saeb, M., Elmessiery, M. and Badawi, U. (2003), 'A hybrid hiding encryption algorithm (HHEA) for data communication security', *Proceedings of 2003 IEEE 46th Midwest Symposium on Circuits and Systems*, Cairo, Egypt, pp. 476-478.

Tat Wi, C. (2010), 'Implementation of hybrid encryption method using Caesar cipher algorithm', Unpublished master thesis, University Malaysia Pahang (UMP), Pahang, Malaysia.

About the authors

Prakash Kuppuswamy, Lecturer, Computer Engineering & Networks Department in Jazan University, KSA. He is research Scholar-Doctorate Degree yet to be awarded by "Dravidian University." He has published 15 International Research journals/Technical papers and participated in many international conferences in Rep. of Maldives, Libya and Ethiopia. His research area includes Cryptography, Bio-informatics and Network algorithms.

Corresponding author. College of Computer Science & Information System, Jazan University (PO BOX 114, Jazan, Saudi Arabia, KSA). Tel: +966-532883941. E-mail address: prakashcnet@gmail.com

Saeed Q. Y. Al-Khalidi, Dean, Deanship of Libraries Affairs at King Khalid University, Abha. KSA. He published many National & International papers, Journals. Also, he participated as a Reviewer in many international conferences worldwide. He completed Master Degree and Doctor of Philosophy in University of East Anglia. His research interests include: Information System development, approaches to systems analysis and the early stages of systems development process, IT/IS evaluation practices, E-readiness assessment. E-mail address: salkhalidi@yahoo.com