International Journal for Modern Trends in Science and Technology, 8(09): 302-306, 2022

ISSN: 2455-3778 online
DOI: https://doi.org/10.46501/IJMTST0809058
Available online at: http://www.ijmtst.com/vol8issue09.html

A Dynamic Permutation-Based Symmetric-Key Encryption Scheme

B Susheel Kumar, N Raja Rajeswari, P Krishnaiah, Venkata Narayana Reddy

Department of Computer Science and Technology, Yogi Vema University, Kadapa, India.

To Cite this Article
B Susheel Kumar, N Raja Rajeswari, P Krishnaiah and Venkata Narayana Reddy. A Dynamic Permutation-Based Symmetric-Key Encryption Scheme. *International Journal for Modern Trends in Science and Technology* 2022, *8(09)*, pp. 302-306. https://doi.org/10.46501/IJMTST0809056

Article Info
Received: 03 September 2022; Accepted: 24 September 2022; Published: 28 September 2022.

ABSTRACT

Cryptography is the investigation of securing figuring assets in an open interconnected conveying framework. Abstract - Data are some of the most valuable assets and need to be protected to prevent theft, compromise, or inappropriate use. The data protection can be achieved by the security. Security breaches occur for a variety of reasons and victims range from smallest of businesses to the largest of public agencies. Security is the state of being free from danger or threat. In this paper an information security method proposed to provide much security to sensitive data with small key with permutation choice. The sensitivity analysis and validation are conducted further. Finally, an example is given to illustrate the application of the proposed method.

Keywords: Cryptography, Sensitive data, Security, Protection.

I. INTRODUCTION

Data are some of the most valuable assets and need to be protected[3][4] to prevent theft, compromise[1][2], or inappropriate use. The data protection can be achieved by the security. Security breaches occur for a variety of reasons and victims range from smallest of businesses to the largest of public agencies.

This paper discusses the need for, and the possibility of, a shared definition of security. This is done by investigating the concept of security [6][7] in the areas of international relations, crime prevention, risk management, and loss prevention. In particular, it discusses to what extent a common framework of understanding can be applied to investigate the concept in the different areas. One is offered for analysis and discussion.

The following images illustrate different threats:

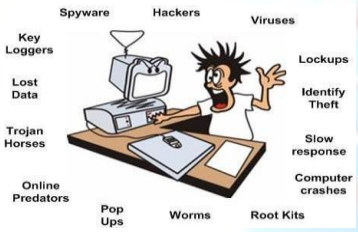


Figure 1: Different Possible Threats

Figure 2: Password Cracking

II. INFORMATION ASSETS

In this context, information assets refer to documents that contain vital data related to business. Where hardcopy once dominated, information is now stored and managed as data that is easily shared with customers, vendors, clients, and colleagues by emails, shared folders, web download, handheld devices etc. The widespread access to the Internet, the digital information is far more convenient and cost-effective to share and manage. This has dramatically improved workgroup productivity by facilitating collaboration and improving response time to customers, clients and others. However this welcome convenience has increased risk of unauthorized disclosure, transfer, modification, or destruction of information – whether accidental or intentional.

The following figure illustrates various information assets:

Figure 3: Information Assets

III. SERVICES OF SECURITY

The following are the services of information security:

- Confidentiality
- Integrity
- Authentication
- Non-repudiation

Cryptography offers confidentiality and integrity of messages. Confidentiality ensures no one else can read your messages unless they have knowledge of the decryption key.Integrity [9] knows the message is unaltered, and can be performed with either a trusted third party, hashing algorithm, or with public key cryptography [3][4][6].

IV. WHICH SECURITY SERVICE DOES ENCRYPTION PROVIDE?

It encrypts [2][5] data so that the content is not visible to unauthorized people – it primarily provides the service of 'Confidentiality'. Since meaning-full changes cannot be made without the appropriate decryption key, and data checksums can be encrypted to provide signatures it can also help to obtain both 'Integrity' and 'Non-repudiation'.

V. NEED OF SECURITY

Ensuring that your information remains confidential and only those who *should* access that information *can*.

Knowing that no one has been able to change your information, so you can depend on its accuracy (information integrity). Making sure that your information is available when you need it (by making back-up copies and, if appropriate, storing the back-up copies off-site).

VI. PROPOSED METHOD

The proposed method consists of the following methods:

- Key Generation
- Encryption
- Decryption
- Round Function

1. Key Generation

For each round two 4-bit keys selected from 128-bit random key. Key selector selects two 4-bit keys from 32 4-bit(128-bit random key) words using permutation choice. After 16-rounds permutation changed one position in circular manner. The key generation process illustrated in the following Figure 4:

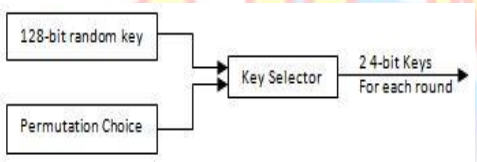


Figure 4: Key Generation Process

2. Encryption

The plain text (8-bit) divided into two halves, each halve individually processed. Each round uses two 4-bit keys and produces 8-bit output. Each 8-bit plain text processed in sixteen rounds to produce corresponding 8-bit cipher text. The following Figure 5 illustrates the encryption process:

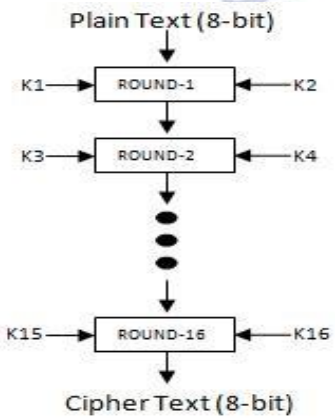


Figure 5: Encryption Process

3. Decryption

The cipher text (8-bit) divided into two halves, each halve individually processed. Each round uses two 4-bit keys and produces 8-bit output. Each 8-bit plain text processed in sixteen rounds to produce corresponding 8-bit plain text. The keys are used reverse to the encryption process: The following Figure 6 illustrates the decryption process:

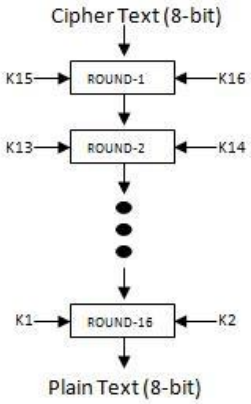


Figure 6: Decryption Process

4. Round Function for Encryption

The left halve and key k1 given as input to exclusive-or. The right halves shifted (circular left shift) previous output number of times. The output of previous step XORed with key k2. The right halve output shifted (circular left shift) right halve exclusive-or output number of times. Finally, two halves swapped .The output of each round given as input to next round. The round function for encryption [9] illustrated in the following Figure 7.

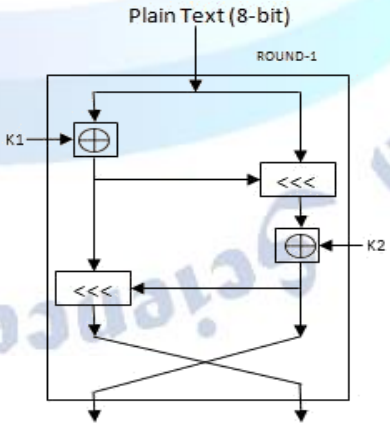


Figure 7: Encryption Round Function

5. Round Function for decryption

The left halve and key k15 given as input to exclusive-or. The right halves shifted (circular right shift)[10] previous output number of times. The output of previous step

XORed with key k16. The right halve output shifted (circular right shift) right halve exclusive-or output number of times. Finally, two halves swapped .The output of each round given as input to next round. The round functions for encryption illustrated in the following Figure 8.

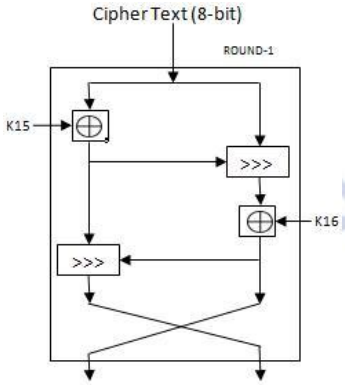
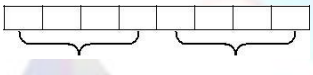


Figure 8: Decryption Round Function

VII. EXAMPLE

Let, the character is —T‖. Now according to steps we will get the following: ASCII of —T‖ is 84 in decimal. The binary value of 84 is 1010100. Since it is not 8-bit binary number we need to make it 8-bit number as per the encryption algorithm. So it would be 01010100.



0 1 0 1 0 1 0 0

Left Halve (LH) Right Halve (RH)

128-bit key(32 4-bit words)

A	F	B	C	E	B	1	4
9	D	E	7	E	F	D	5
8	E	B	A	D	9	3	9
C	6	A	D	6	F	D	F

K2

K

Permutation choice (Unique Values)

10	8	1	20	26	9	29	32
11	15	5	18	12	17	4	22
24	7	13	23	2	14	31	27
3	16	21	6	19	25	28	30

k1=D => k1=1101 and

k2=4 => k2=0100

1) LH=LH ⊕k1=0101 ⊕1101=1000

RH=RH<<<(LH ⊕k1)
=0100<<<1000 =0100
3) RH=RH ⊕k2=0100 ⊕0100=0000
4) LH=LH<<<RH=1000<<<0000
=1000

5) Swap LH and RH
LH=0000 and RH=1000
6) Output = 00001000

We repeat the above procedure for all rounds.

VIII. ADVANTAGES OF THE NEW ALGORITHM

1. The algorithm is very simple in nature
2. There are two operations in each round in this algorithm which would make it more secured.
3. For any amount of data this algorithm will work smoothly.
4. The algorithm more secure with small key size that is possible with permutation choice.
5. The algorithm is very fast with simple operation
6. The analysis of algorithm is very easy with its simple in nature.

IX. FUTURE WORK

The paper analyses of the original and optimized algorithms suggest that there is more opportunity to improve the performance of cryptographic process. The algorithm allows extending block size, key size and permutation choice with miner modification.

X. CONCLUSION

The follow-on accomplishment of the projected cryptographic system is proved safe and sound against attacks. In the beam of every part of above ponder and examination, this revision suggests the obligatory of randomness in key to get optimal encryption security. To select lengthy key means just to increase the processing time, wastages of extra memory and electric power. There is more opportunity to improve the performance.

REFERENCES

[1] Alireza jolfaei , Xin-Wen Wu, Vallipuram Muthukkumarasamy "On the Security of Permutation-only Image Encryption Schemes" IEEE transactions on information forensics and security (volume: 11, issue: 2, feb. 2016), 235 - 246

[2] M. Basu, B. Prasad, The generalized relations among the code elements for Fibonacci coding theory, Chaos Solitons Fractals 41 (2009), no. 5, 2517–2525.

[3] Dr. V. Sundaram, —Secured Communication through FibonacciNumbers and Unicode Symbols" International Journal of Scientific& Engineering Research, Vol. 3, Issue 4, April 2012, pp. 490-494.

[4] Ahmad Abusukhon, Mohamad Talib, Issa Ottoum, "Secure Network Communication Based on Text – to –Image Encryption" International Journal of Cyber - Security and Digital Forensics(IJCSDF), 2012, pp. 263-271

[5] L. B. Milstein et al., —On the feasibility of a CDMA overlay for personal communications networks,‖ IEEE J. Selecred Areas Commun., vol. 10, pp. 655-668, May 1992.

[6] D. K. Sarmah and N. bajpai, —Proposed system for data hhid-ing using cryptography and steganography, International Journal of Computer Applications (0975– 8887), vol. 8, no. 9, October 2010.

[7] B. S. Tarle, G. L. Prajapati, On the information security using Fibonacci series, International Conference and Workshop on Emerging Trends in Technology (ICWET 2011)-TCET, Mumbai, India.

[8] Fakariah Hani Mohd Ali, Ramlan Mahmod, Mohammad Rushdan and Ismail Abdullah, "A Faster Version ofRijndael Cryptographic Algorithm Using Cyclic Shift and Bit Wise Operations", International Journal of Cryptology Research pp: 215-223 (2009).

[9] Wadi, S., M., Zainal, N.A. low cost implementation of Advanced Encryption Standard algorithm using 8085A microprocessor. 3rd international technical conference (ITC2012),2012, pp. 157-163

[10] AbdElHaleem SH, Radwan AG, Abd-El-Hafiz SK. A chess-based chaotic block cipher. In: IEEE international new circuits and system conference (NEWCAS); 2014. p. 405–8.