ISSN No. 0976-5697

Volume 8, No. 5, May – June 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Vantages of Adaptive Multidimensional Playfair Cipher over AES-256 and RSA-2048

Krishnaraj Bhat, Dindayal Mahto and Dilip Kumar Yadav
Department of Computer Applications
National Institute of Technology
Jamshedpur, India

Abstract: Adaptive Multidimensional Playfair Cipher (AMPC) has the capacity to provide secrecy to all kinds of data. The primary objective of this research is to compare this cipher with the standard ciphers AES-256 and RSA-2048, and find the advantages of AMPC over them. The comparisons are done on the basis of encryption and decryption times, plain data size versus cipher data size, possible number of keys and types of data supported. It is found from the comparison analysis that the AMPC is more efficient in terms of memory and bandwidth utilization when compared to the standard ciphers. AMPC and RSA-2048 are always unambiguous whereas in case of AES-256, data size has to be a multiple of 16 bytes or padded values shouldn't be a part of original data values in order to be unambiguous. Also, AES-256 is very weak against brute force attack when compared to other two ciphers. Among AMPC and RSA-2048, former is more efficient in terms of time, memory and bandwidth. Therefore, applications desiring to secure all types of data unambiguously and efficiently with respect to memory and bandwidth consumption irrespective of data size can use AMPC.

Keywords: Data security; Cryptography; AES; RSA; Playfair cipher

I. INTRODUCTION

Nowadays, confidential data to be carried via internet exist in different forms such as text, image, audio, video, encoded, compressed etc. Since internet is an open architecture it is prone to attacks. Hence, the confidential data have to be carried in the opaque form. One of the ways to achieve this is by using cryptography. AES and RSA are the two standard symmetric and asymmetric ciphers respectively that are used for encryption and decryption of data in today's world [1], [2]. But, both have pros and cons. AMPC can secure all kinds of data [3]. AES, RSA and AMPC are introduced in the following subsections.

A. AES

NIST determined to form an successor of DES after some security defects in DES in 1997. Two conferences were held (AES1 in August 1998 and AES2 in March 1999) and the purpose was not only the security but also the performance in different aspects of settings. In October 2000, Rijndael algorithm for encryption/decryption was chosen and after long security and performance testing, got approved by the U.S government in 2001 [4]. The AES was published in 2001 by NIST as the symmetric block cipher algorithm and became the successor of DES as accepted standard. In AES, block size is 128 bits for both hardware and software implementations [5]. AES block size is fixed i.e. 128 bits and key sizes can be 128 or 192 or 256 bits. But, Rijndael's block sizes and key sizes are multiple of 32 bits with a minimum of 128 bits [6]. The block sizes have a limitation of 256 bits but key sizes are not fixed theoretically. There has been attack on 7 rounds for 128-bit, 8 rounds for 192-bit and 9 rounds for 256-bit keys [7]. Hence, AES has 10, 12 and 14 rounds for key sizes 128, 192 and 256 bits respectively. AES is highly structured and efficient algorithm to protect the confidential information at the most prominent secure level [8].

B. RSA

Reference [9] gives the complete working of RSA which is considered as the first real life and practical asymmetric key cryptosystem. It becomes de facto standard for public key cryptography. Its security lies in the integer factorization problem. For strong security of data, large cryptographic keys (public key and private key) are required. Since the keys till size 768 bits are already broken and 1024 bits key can be broken in this decade, 2048 bits key is used worldwide [10].

C. Adaptive Multidimensional Playfair Cipher (AMPC)

It is a novel extension of the Classical Playfair cipher, supporting the security of 256 values from 0 to 255 which can be stored in a byte memory due to which it can support the security of all kinds of information. It uses the eight dimensional key matrix of size $2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2$. This cipher has mainly three steps for encryption: XORing of values, columnar rotation of values and multidimensional Playfair cipher encryption which are repeated ten times [3]. This cipher removes the limitation of four dimensional Playfair cipher fused with Linear Feedback Shift Register which consumes more memory and bandwidth [11], [12]. AMPC uses the idea given in the generalization for multidimensional playfair cipher [13] to perform multidimensional encryption/decryption. AMPC has been found as the best variant in terms of security, and memory and bandwidth consumption among existing Playfair cipher variants [3].

The main intention of this research is to find the vantages of AMPC over the standard ciphers AES-256 and RSA-2048. Section II provides the comparison analysis of the three ciphers in which it is detected that applications to be developed with a purpose of securing all types of data unambiguously and efficiently in terms of memory and bandwidth irrespective of data size can use AMPC.

II. COMPARISON ANALYSIS

The ciphers AES-256, RSA-2048 and AMPC are implemented using C programming and executed in a computer machine having 64-bit processor with 2.16GHz speed, 2GB RAM and Ubuntu 16.0 operating system. GMP (GNU Multi Precision) library is used for developing RSA-2048. Test data used are of sizes 5, 50, 500, 5000 and 50000 bytes. The comparisons are shown in the following subsections which are made on the basis of encryption and decryption times, plain data size Vs cipher data size, possible number of keys and types of data supported.

A. *Encryption and Decryption Times*

Table I shows the times taken by the three ciphers for encryptions and decryptions of different data sizes. It can be seen that RSA-2048 cipher takes more time in each case than the other two ciphers. AES-256 cipher takes the least amount of time for both encryption and decryption of each data size. Second best is the AMPC.

Table I. Encryption and decryption times for different data sizes

Cipher	*5 bytes*		*50 bytes*		*500 bytes*		*5,000 bytes*		*50,000 bytes*	
	Enc. time (µs)	*Dec. time (µs)*	*Enc. time (µs)*	*Dec. time (µs)*	*Enc. time (µs)*	*Dec. time (µs)*	*Enc. time (µs)*	*Dec. time (µs)*	*Enc. time (µs)*	*Dec. time (µs)*
AES-256	11	13	38	50	300	393	2,895	3,777	30,107	40,028
RSA-2048	133	75,808	1,259	758,122	12,508	7,553,984	124,634	75,920,404	1,280,373	779,877,935
AMPC	8	6	66	64	602	604	5,827	5,848	59,491	59,991

B. *Plain Data Size Vs Cipher Data Size*

Table II shows the cipher data sizes produced by the three ciphers for different plain data sizes. It can be seen that AMPC is the efficient one and RSA-2048 is the inefficient one with respect to memory and bandwidth consumption. AES-256 is the second efficient cipher.

Table II. Cipher data sizes for different plain data sizes

Plain data size (in bytes)	*Cipher data size (in bytes)*		
	AES-256	*RSA-2048*	*AMPC*
5	16	1,280	5
50	64	12,800	50
500	512	1,28,000	500
5,000	5,008	1,280,000	5,000
50,000	50,000	12,800,000	50,000

C. *Possible Number of Keys*

Stronger is the cipher against brute force attack when number of possible keys is more. Table III shows the possible number of keys for each cipher. Here, RSA-2048 has the highest number. It is the possible number of (p, q) pairs where p and q are two unequal primes. AMPC is second in line whose possible number of keys is calculated by taking the factorial of number of values it supports which is the factorial of 256. For AES-256, it is 2^{256} which is the least.

Table III. Possible number of keys for AES-256, RSA-2048 and 4D Playfair cipher fused with LFSR

Cipher	*Possible number of keys*
AES-256	1.1×10^{77}
RSA-2048	5.8×10^{613}
AMPC	8.5×10^{506}

D. *Types of Data Supported*

A cipher is said to be ambiguous if it is unable to decide whether a padded or filler value in the decrypted data is a part of the original data or not. RSA-2048 and AMPC can unambiguously secure all types of data. Since any message can be represented in the form of bytes, RSA-2048 encrypts/decrypts each byte value separately and AMPC encrypt/decrypt byte values within a block where a block can have maximum of 2048 values and minimum of 1 value depending on the message size making it unambiguous. AES-256 works with 16 bytes of data at once. Even though the plain data size is not a multiple of 16, it is made one by appending padding bytes at the end of the plain data and then encrypted. For AES-256, in order to be unambiguous, data size has to be a multiple of 16 bytes or padded byte values shouldn't be a part of original data values. The summary is shown in Table IV.

Table IV. Types of data supported

Cipher	*Types of data*
AES-256	Data size has to be a multiple of 16 bytes or padded values shouldn't be a part of original data values in order to be unambiguous
RSA-2048	All types of data
AMPC	All types of data

III. CONCLUSION

It can be seen from the comparison analysis that AES-256 is efficient in terms of time. But, AES-256 will be ambiguous if data size is not a multiple of 16 bytes or padded values are a part of original data values. Also, AES-256 is weak against brute force attack when compared to other two ciphers. Even though RSA-2048 is the strongest in terms of brute force attack and can secure all kinds of data unambiguously, it is highly time, memory and bandwidth inefficient. Hence, AMPC can be used to secure all sorts of data efficiently with respect to memory and bandwidth, and unambiguously irrespective of data size.

IV. REFERENCES

[1] S. K. Rao, D. Mahto and D. A. Khan, "A Survey on Advanced Encryption Standard", International Journal of Science and Research, vol. 6, no. 1, Jan. 2017, pp. 711-724, DOI: 10.21275/ART20164149.

[2] D. Mahto, D. A. Khan and D. K. Yadav, "Security Analysis of Elliptic Curve Cryptography and RSA", Proceedings of the World Congress on Engineering, vol. 1, Jun. – Jul. 2016.

[3] K. Bhat, D. Mahto and D. K. Yadav, "Information Security using Adaptive Multidimensional Playfair Cipher", International Journal of Advanced Research in Computer Science, vol. 8, no. 4, May-June 2017.
[4] J. Nechvatal, E. Barker, L. Bassham, W. Burr, M. Dworkin, J. Foti and E. Roback, "Report on the development of the Advanced Encryption Standard (AES)", National Institute of Standards and Technology , Oct. 2000.
[5] B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, N. Ferguson, T. Kohno and M. Stay, "The Twofish Team's Final Comments on AES Selection", May 15, 2000.
[6] J. Daemen and V. Rijmen, "AES proposal: Rijndael", 1999.
[7] J. Daemen and V. Rijmen, "Advanced Encryption Standard", Proceedings of Federal Information Processing Standards Publications, National Institute of Standards and Technology, 2001, pp. 19-22.
[8] D. Selent, "Advanced Encryption Standard", Rivier Academic Journal, vol. 6, no. 2, 2010.
[9] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", Commun. ACM, vol. 21, no. 2, Feb. 1978, pp. 120–126.
[10] D. Fisher, "Experts debate risks to crypto", E-Week, March 27, 2002.
[11] K. Bhat, D. Mahto and D. K. Yadav, "A Novel Approach to Information Security using Four Dimensional (4D) Playfair Cipher fused with Linear Feedback Shift Register", Indian Journal of Computer Science and Engineering, vol. 8, no. 1, Feb-March 2017, pp. 15-32.
[12] K. Bhat, D. Mahto and D. K. Yadav, "Comparison Analysis of AES-256, RSA-2048 and Four Dimensional Playfair Cipher Fused with Linear Feedback Shift Register", International Journal of Advanced Research in Computer Science, vol. 8, no. 3, March-April 2017, pp. 420-422.
[13] K. Bhat, D. Mahto and D. K. Yadav, "Generalization for Multidimensional Playfair Cipher", International Journal of Advanced Research in Computer Science, vol. 8, no. 3, March-April 2017, pp. 379-381.