# AN ENHANCED BLOWFISH ALGORITHM BASED ON CYLINDRICAL COORDINATE SYSTEM AND DYNAMIC PERMUTATION BOX

**ASHWAK MAHMOOD ALABAICHI**

**DOCTOR OF PHILOSOPHY**
**UNIVERSITI UTARA MALAYSIA**
**2014**

# Permission to Use

In presenting this thesis in fulfilment of the requirements for a postgraduate degree from Universiti Utara Malaysia, I agree that the Universiti Library may make it freely available for inspection. I further agree that permission for the copying of this thesis in any manner, in whole or in part, for scholarly purpose may be granted by my supervisor(s) or, in their absence, by the Dean of Awang Had Salleh Graduate School of Arts and Sciences. It is understood that any copying or publication or use of this thesis or parts thereof for financial gain shall not be allowed without my written permission. It is also understood that due recognition shall be given to me and to Universiti Utara Malaysia for any scholarly use which may be made of any material from my thesis.

Requests for permission to copy or to make other use of materials in this thesis, in whole or in part, should be addressed to:

Dean of Awang Had Salleh Graduate School of Arts and Sciences
UUM College of Arts and Sciences
Universiti Utara Malaysia
06010 UUM Sintok

# Abstrak

Algoritma Blowfish (BA) adalah sifer blok simetri yang menggunakan rangkaian *Feistel* untuk melakukan fungsi penyulitan dan penyahsulitan yang mudah. Kunci BA adalah pelbagai dari bit 32 ke 448 untuk memastikan tahap keselamatan yang tinggi. Walau bagaimanapun, kotak penggantian (Kotak-S) dalam BA mengambil peratus ruang memori yang tinggi dan mempunyai masalah keselamatan, terutamanya dalam kerambangtarikan output bagi teks dan fail imej yang mempunyai rentetan besar dan mempunyai bait yang serupa. Dengan demikian, objektif kajian ini adalah untuk mempertingkatkan BA bagi mengatasi masalah ini. Kajian ini melibatkan tiga fasa; reka bentuk algoritma, pelaksanaan, dan penilaian. Dalam fasa reka bentuk, Kotak-S 3D dinamik, Kotak Pilih Atur (Kotak-P) dinamik, dan Fungsi Feistal (Fungsi-F) direkabentuk. Pembaikan ini melibatkan integrasi sistem koordinat silinder (CCS) dan Kotak-P dinamik. BA yang dipertingkatkan dikenali sebagai algoritma Ramlan Ashwak Faudziah (RAF). Fasa pelaksanaan melibatkan pengembangan kunci, penyulitan data, dan penyahsulitan data. Fasa penilaian meliputi mengukur algoritma dari segi memori dan keselamatan. Dari segi memori, keputusan menunjukkan RAF menggunakan 256 bait, iaitu kurang daripada BA (4096 bait). Dari segi kerambangtarikan pada teks dan fail imej yang mempunyai rentetan besar dan mempunyai bait yang serupa, kadar purata kerambangtarikan untuk 188 ujian statistik memperolehi nilai lebih daripada 96%. Ini bermakna RAF mempunyai kerambangtarikan tinggi yang menunjukkan bahawa ianya lebih terjamin. Dengan demikian, keputusan ini menunjukkan bahawa algoritma RAF yang mengintegrasikan CCS dan dinamik Kotak-P adalah satu pendekatan berkesan yang dapat mengurangkan ingatan dan mengukuhkan keselamatan.

**Kata kunci**: Sistem Koordinat Silinder, Kotak-S dinamik, Kotak-P dinamik, Algoritma Blowfish

# Abstract

The Blowfish Algorithm (BA) is a symmetric block cipher that uses Feistel network to iterate simple encryption and decryption functions. BA key varies from 32 to 448 bits to ensure a high level of security. However, the substitution box (S-Box) in BA occupies a high percentage of memory and has problems in security, specifically in randomness of output with text and image files that have large strings of identical bytes. Thus, the objective of this research is to enhance the BA to overcome these problems. The research involved three phases, algorithm design, implementation, and evaluation. In the design phase, a dynamic 3D S-Box, a dynamic permutation box (P-Box), and a Feistal Function (F-Function) were improved. The improvement involved integrating Cylindrical Coordinate System (CCS) and dynamic P-Box. The enhanced BA is known as Ramlan Ashwak Faudziah (RAF) algorithm. The implementation phase involved performing key expansion, data encryption, and data decryption. The evaluation phase involved measuring the algorithm in terms of memory and security. In terms of memory, the results showed that the RAF occupied 256 bytes, which is less than the BA (4096 bytes). In terms of randomness of text and image files that have large strings of identical bytes, the average rate of randomness for 188 statistical tests obtained values of more than 96%. This means that the RAF has high randomness indicating that it is more secured. Thus, the results showed that the RAF algorithm that integrates the CCS and dynamic P-Box serves as an effective approach that can consume less memory and strengthen security.

**Keywords**: Cylindrical Coordinate System, Dynamic 3D S-Box, Dynamic P-box, Blowfish Algorithm.

# Acknowledgement

First of all I have to express my thanks and gratitude to Allah who gives me the ability to achieve this imperfect work and without his blessing and support nothing can be done.

I would like to thank my supervisors, advisors Prof. Dr. Ramlan Mahmod and Associate Prof. Dr. Faudziah Ahmad for their continuous support during my Ph.D. program.

Special thanks goes to my colleague Mohammed Sahib Mechee for his continuous support and encouragement along the study and research time.

I would also like to offer my deepest gratitude to my family for helping me, and for encouraging me to do my PHD work which enabled me to successfully accomplish my tasks.

I am deeply indebted to my dear friends and staff in UUM especially from the School of Computing for taking so much time and interest in my work, always being there for me through my difficult situations and spending their time in guiding me despite their busy schedule.

Last but not least, thanks to all those who have been directly and indirectly involved in helping me complete this research.

Finally, I apology to those whose names might be missed. But, I am grateful to all of them for their help and on various matters of day-to-day life.

# Table of Contents

# List of Tables

# List of Figures

# List of Appendices

# List of Publications

ALabiachi, A.., Ahmad, F., & Ku, R.K. (2011). A Conceptual Design of Novel Modern Random Key-Stream Generator for High Immunity Correlation Attack. *2011* UKSim 13th International Conference on Computer Modelling and Simulation, 399–402. doi:10.1109/UKSIM.2011.82.

ALabiachi, A., Ahmad, F., & Ku, R.K. (2011). A Competitive Study of Cryptography Techniques over Block Cipher. *2011* UKSim 13th International Conference on Computer Modelling and Simulation, 415–419. doi:10.1109/UKSIM.2011.85.

ALabaichi, A., Mahmod, R., & Ahmad, F. (2013). Randomness Analysis on Blowfish Block Cipher. AWERProcedia Information Technology & Computer Science: 3rd World Conference on Innovation and Computer Science (pp. 1115-1127), Antalya, Turkey.

ALabaichi, A.., Mahmod, R., Ahmad, F., & Mechee, M. (2013).Randomness Analysis on Blowfish Block Cipher using ECB and CBC Modes. Journal of Applied sciences, *13*(5), 758-789.

ALabaichi, A., Mahmod, R., & Ahmad, F. (2013). Analysis of Some Security Criteria for S-Boxes in Blowfish Algorithm. International Journal of Digital Content Technology and its Applications (JDCTA), *7*(12), 8–20.

ALabaichi, A., Mahmod, R., & Ahmad, F. (2013). Security Analysis of Blowfish Algorithm. Proceding of SDIWC: The Second International Conference on Informatics & Applications on IEEE (pp.12–18).

ALabaichi, A., Mahmod, R., & Ahmad, F. (2013). Randomness Analysis of 128 bits Blowfish Block Cipher on ECB mode. (IJCSIS) International Journal of Computer Science and Information Security, 11 (10), 8-21.

ALabaichi, A., Mahmod, R., & Ahmad, F. (2014). A Cylindrical Coordinate System with Dynamic Permutation Table for Blowfish Algorithm. International Journal of Soft Computing 5(9).

ALabaichi, A., Mahmod, R., & Ahmad, F. (2013). Randomness Analysis of 128 bits Blowfish Block Cipher on ECB and CBC Modes, International Journal of Digital Content Technology and its Applications (JDCTA), 7(15), 77-89.

ALabaichi, A., Mahmod, R, Ahmad, F., (2014). A dynamic 3D S–Box based on Cylindrical Coordinate System for Blowfish Algorithm. The 3rd International Conference on Computer Science & Computational Mathematics (ICCSCM 2014). Langkawi, Malaysia, ISBN: 978-967-11414-6-5.

# List of Abbreviations

| | |
|---|---|
| RSA | Rivest – Shamir - Adleman |
| AES | Advance Encryption Standard |
| BA | Blowfish Algorithm |
| DES | Data Encryption Standard |
| 3DES | Triple Data Encryption Standard |
| IDEA | International Data Encryption Algorithm |
| RC5 | Rivest Cipher 5 |
| RC4 | Rivest Cipher 4 |
| S-Box | Substitution box |
| P-Box | Permutation box |
| CCS | Cylindrical Coordinate System |
| CCSDPB | Cylindrical Coordinate System and Dynamic Permutation Box |
| RAF | Ramlan – Ashwak - Faudziah |
| 3D | Three Dimensional |
| 2D | Two Dimensional |
| XOR | Exclusive OR |
| SPN | Substitution - Permutation Network |
| NIST | National Institute of Standard and Technology |
| ECB | Electronic Codebook Mode |
| CBC | Cipher Block Chaining Mode |
| CFB | Cipher Feedback Mode |
| OFB | Output Feedback Mode |
| CTR | Counter Mode |
| DSDP | Key-Dependent S-Box and Key-Dependent P-Boxes |
| VMS-AES | Variable Mapping Substitution - Advance Encryption Standard |
| SK | Secret Key |
| LFSR | Linear Feedback Shift Register |
| PN | Pseudo Number |
| SKs | Secret Keys |
| Eks | Encryption keys |
| P-value | Probability value |
| AVAL | Avalanche Criterion |
| SAC | Strict Avalanche Criterion |
| BIC | Bit Independence Criterion |
| KP | Known Plaintext |
| LC | Linear Cryptanalysis |
| BR | Byte Relocation |
| BT | Byte Transformation |
| PRT | Partial Round Test |
| FRT | Full Round Test |
| BBS | Blum-Blum-Shub |

# CHAPTER ONE

# INTRUDUCTION

## 1.1 Background

The advancements in technologies have changed the way people communicate with each other. Technologies have accelerated communications, resulting in an exponential information exchange, especially in digital landscape. Hence, it allows people, regardless of the places they are at and the time zone they are in to communicate and transfer information extensively in a borderless manner. In this kind of situation, the protection of transmitted data is very important. This is because in such landscape, the possibility of data theft is high, and eventually results in data loss. More importantly, the attacked data could be manipulated by the attackers for undesirable purposes (Verma, Agarwal, Dafouti, & Tyagi, 2011).

In order to ensure that transmitted data are safe, cryptography has been popularly used Rolf (2005). Cryptography techniques encrypt and hide information. This means that the original information will not been tampered and the information can only be accessed in pieces and not as a whole (Menezes, Van Oorschot, & Vanstone, 1997).

Existing popular cryptographic algorithms on block cipher include DES, RC2, IDEA, CAST, Rijndael, Twofish, RC6, MARS, Serpent, and Blowfish. The limitations of these algorithms except Blowfish are not highly secured and slow.

As mentioned, one of the popular cryptographic algorithms is the Blowfish Algorithm (BA). BA is a symmetric-key block cipher, designed in 1993 by Bruce Schneier and

# REFERENCES

Abd-ElGhafar, A. R., Diaa, A., Rohiem, A., & Mohammed, F. (2009). Generation of AES Key Dependent S-Boxes using RC4 Algorithm. *13th International Conference on Aerospace Sciences & Aviation Technology* (pp. 26-28).

Acharya, T., & Ray, A. K. (2005). *Image processing: principles and applications*: John Wiley & Sons.

Adams, C., & Tavares, S. (1990). The structured design of cryptographically good S-Boxes. *journal of Cryptology*. *Springer,3*(1), 27-41.

Agrawal, H., & Sharma, M. (2010). Implementation and analysis of various symmetric cryptosystems. *Indian Journal of Science and Technology*, *3*(12), 1173-1176.

Ariffin, S. (2012). *A Human Immune System Inspired Byte Permutation Of Block Cipher*. Doctoral dissertation. Universiti Putara Malaysia.

Ahmed, N. (n.d.). Testing an S-Box for Cryptographic Use. *International Journal of Computer and Electrical Engineering*.

ALabaichi, A. M., Mahmod, R., & Ahmad, F. (2013a). Randomness Analysis on Blowfish Block Cipher. *AWERProcedia Iinformation Technology & Computer Science: 3rd World Conference on Innovation and Computer Science* (pp. 1116-1127), Antalya, Turkey.

ALabaichi, A. M., Mahmod, R., Ahmad, F., & Mechee, M.S. (2013b). Randomness Analysis on Blowfish Block Cipher using ECB and CBC Modes, 2013, *Journal of Applied Sciences,13*(6),768-789.

ALabaichi, A., Mahmod, R., & Ahmad, F. (2013c). Analysis of Some Security Criteria for S-Boxes in Blowfish Algorithm, *International Journal of Digital Content Technology and its Applications (JDCTA*), *7*(12), 8–20.

ALabaichi, A. M., Mahmod, R., & Ahmad, F. (2013d). Security Analysis of Blowfish algorithm. *Proceding of SDIWC: The Second International Conference on Informatics &Applications on IEEE* (pp.12–18), lodz university of tehnolgoy .

ALabaichi, A., Mahmod, R., & Ahmad, F. (2013e). Randomness Analysis of 128 bits Blowfish Block Cipher on ECB mode. *(IJCSIS) International Journal of Computer Science and Information Security*, *11* (10), 8-21.

ALabaichi, A., Mahmod, R., & Ahmad, F. (2013f). Randomness Analysis of 128 bits Blowfish Block Cipher on ECB and CBC Modes. *International Journal of Digital Content Technology and its Applications (JDCTA*), 7(15), 77-89.

Alani, M. d M. (2010). Testing randomness in ciphertext of block-ciphers using dieHard tests. *International Journal of Computer Science and Network Security, 10* (4), 53-57.

Al-Hazaimeh, O. M. A. (2010). *New Cryptographic Algorithms for Enhancing Security of Voice Data*. Doctoral dissertation. Universiti Utara Malaysia.

Ali, F.H.M. (2009). *A NEW 128-BIT BLOCK CIPHER*. Doctoral Dissertation. Universiti Putra Malaysia.

Ali, N. B. Z., & Noras, J. M. (2001). Optim al Datapath Design for a Cryptographic Processor: The Blowfish Algorithm. *Malaysian Journal of Computer Science. Faculty of Computer Science and Information Technology, 14*(1), 16-27.

Ali, S.A. (2005*). Improving the Randomness of Output Sequence for the Advanced Encryption Standard Cryptographic Algorithm*. Master thesis. Universiti Putra Malaysia.

Al-Neaimi, A. M. A., & Hassan, R. F. (2011a). New Approach for Modified Blowfish Algorithm Using 4-States Keys. *The 5th International Conference on Information Technology* (pp.1-4).

Al-Neaimi, A. M. A., & Hassan, R. F. (2011b). New Approach for Modifying Blowfish Algorithm by Using Multiple Keys. *International Journal of Computer Science and Network Security (IJCSNS), 11*(3), 21-26.

Alsultanny, Y. A., & Jarrar, H. J. (2006). Generating and testing random key for image encryption using ECB and CBC modes. *Jordan Journal of Applied Science Natural Sciences*. *Deanship Of Scientific Research Applied Science University, 8*(1), 1-11.

Ayoub, F. (1982). Probabilistic completeness of substitution-permutation encryption networks. *IEE Proceedings E (Computers and Digital Techniques), 129*(5), 195-199.

Babbage, S., Canniere, C., Canteaut, A., Cid, C., Gilbert, H., Johansson, T., & Robshaw, M. (2008).

Bagad, V.S. and A.I. Dhotre (2008). *Cryptography and Network Security*. 2nd Revised Edn., Technical Publications, Pune, India.

Berbain, C., Billet, O., Canteaut, A., Courtois, N., & Gilbert, H. (2008). SOSEMANUK , a fast software-oriented stream cipher, 16–18.

Bernstein, D. J. (2008). The Salsa20 family of stream ciphers *New stream cipher designs* (pp. 84-97): Springer.

Bernstein, D. J. (2006). Salsa20/8 and Salsa20/12. *eSTREAM, ECRYPT Stream Cipher Project*.

Biham, E., & Shamir, A. (1993). *Differential cryptanalysis of the full 16-round DES* (pp. 79-88). Springer New York.

Boesgaard, M., Pedersen, T., Vesterager, M., & Zenner, E. (2004). The Rabbit Stream Cipher-Design and Security Analysis. *IACR Cryptology ePrint Archive, 2004,* 291.

Boesgaard, M., Vesterager, M., Pedersen, T., Christiansen, J., & Scavenius, O. (2003). *Rabbit: A new high-performance stream cipher.* Paper presented at the Fast Software Encryption.

Braeken, A. (2006). *Cryptographic properties of Boolean functions and S-Boxes*. Doctoral dissertation. Katholieke Universiteit Leuven.

Brougham, H. P. (n.d.). Coordinate Systems And Transformation, 124–130. Retrieved from http://web.uettaxila.edu.pk/CMS/AUT2012/ectWPAbs/notes%5CLecture%2013%20Notes.pdf

Brannon, R. M. (2004). Curvilinear Analysis in a Euclidean Space. University of New Mexico. Retrieved from http://mech.utah.edu/~brannon/public/curvilinear.pdf

Burwick, C., Coppersmith, D., D'vignon, E., Gennaro, R., Halevi, S., Jutla, C., & Safford, D. (1998). MARS-a candidate cipher for AES. *NIST AES Proposal 268.*

Castro, J. C. H., Sierra, J. M., Seznec, A., Izquierdo, A., & Ribagorda, A. (2005). The strict avalanche criterion randomness test. *Mathematics and Computers in Simulation. Elsevier, 68*(1), 1-7.

Carter, B. A., Kassin, A., & Magoc, T. (2007). Symmetric cryptosystems and symmetric key management. *CiteSeerX, 10*(1.135), 1231.

Chandrasekaran, J., Subramanyan, B., & Raman, G. S. (2011). Ensemble Of Blowfish With Chaos Based S Box Design For Text And Image Encryption. *International Journal of Network Security & Its Applications ( IJNSA). Academy & Industry Research Collaboration Center(AIRCC), 3*(4), 165-173.

Cody, B., Madigan, J., Donald, S.M., & Hsu, K. W. (2007). High speed SOC design for blowfish cryptographic algorithm. In *Very Large Scale Integration. IFIP International Conference on* (pp.284-287). IEEE.

Collins, G. W. (1989). The foundations of celestial mechanics. *The Foundations of Celestial Mechanics, by George W. Collins, II. Tucson, AZ, Pachart Publishing*

*House (Pachart Astronomy and Astrophysics Series. Volume 16), 1989, 158 p., 1*.

Cornwell, J. W. (n.d.). Blowfish Survey. *Department of Computer Science Columbus State University Columbus*, GA. Retrieved from http://cs.columbusstate.edu/cae- ia/StudentPapers/cornwell.jason.pdf

Daemen, J., & Rijmen, V. (2002). *The design of Rijndael: AES-the advanced encryption standard*. Springer.

Dawson, E., Gustafson, H., & Pettitt, A. N. (1992). Strict Key Avalanche Criterion. *Australasian Journal of Combinatorics*, *6*, 147-153.

Deakin, R.E. (2004). Coordinate Transformations In Surveying And Mapping, 1–31. Retrieved from http://user.gs.rmit.edu.au/rod/files/publications/COTRAN_1.pdf

Durstenfeld, R. (1964). ACM Algorithm 235: Random Permutation, *Communications of the ACM,* Vol. 7, No 7.

Denning, D. E.R (1982). *Cryptography and data security*. Addison-Wesley Longman Publishing Co., Inc.

Diffie, W., & Hellman, M. (1976). New directions in cryptography. *Information Theory, IEEE Transactions on*, *22*(6), 644-654.

Doganaksoy, A., Ege, B., Koçak, O., & Sulak, F. (2010). Cryptographic Randomness Testing of Block Ciphers and Hash Functions. *IACR Cryptology ePrint Archive*. 564, 1-12.

Doroshenko, S., Fionov, A., Lubkin, A., Monarev, V., Ryabko, B., & Shokin, Y. I. (2008). Experimental Statistical Attacks on Block and Stream Ciphers. *Computational Science and High Performance Computing III* pp.(155-164) Springer Berlin Heidelberg.

Dworkin, M. (2001). *Recommendation for block cipher modes of operation. methods and techniques* (No.Nist-Sp-800-38a). National Institute Of Standards And Technology Gaithersburg Md Computer Security Div.

Elkamchouchi, H. M., & Elshafee, A. M. (2003). Dynamically key-controlled symmetric block cipher KAMFEE. In *Radio Science Conferenc. NRSC 2003. Proceedings of the Twentieth National* (pp. C19-1). IEEE.

Elkamchouchi, H. M., & Makar, M. A. (2004). Kamkar symmetric block cipher. *Radio Science Conference, 2004. NRSC 2004. Proceedings of the Twenty-First National* (pp. C1-1-C1-9). IEEE.

Elminaam, D., Kader, H. M. A., & Hadhoud, M. M. (2010). Evaluating The Performance of Symmetric Encryption Algorithms. *IJ Network Security*.

Elminaam, D., Kader, H. M. A., & Hadhoud, M. M. (2009). Energy efficiency of encryption schemes for wireless devices. *International Journal of Computer Theory and Engineering, 1*, 302-309.

El-Ramly, S. H., El-Garf, T., & Soliman, A. H. (2001). Dynamic generation of S-Boxes in block cipher systems. *Radio Science Conference, 2001. NRSC 2001. Proceedings of the Eighteenth National* Vol. 2, pp. (389-397). IEEE.

Fahmy, A., Shaarawy, M., El-Hadad, K., Salama, G., & Hassanain, K. (2005). A proposal For A key-dependent AES. *3rd International Conference: Sciences of Electronic, Technologies of Information and Telecommunications. Tunisia: SETIT*.

Feistel, H. (1973). Cryptography and computer privacy. *Scientific American , 228*(5), 15-23.

Gan, L. (2001). A New Stream Cipher.for Secure Digital Media Distribution. Thesis Master of Science (Engineering), Queen's University Kingston, Ontario, Canada.

Gonzales, R. C., & Woods, R. E. (2002). Digital Image Processing. *New Jersey: Prentice Hall*, *6*, 681.

Gill, G.S. (2003).*The calculus bible*. Brigham Young University, Mathematics Department.

Halagali, B. P. (2013). Designing The S Boxes Of Blowfish Algorithm Using Linear Congruential Generator, *ASM's international E-journal of ongoing research in management and IT e-ISSN-2320-0065, V S M Institute of Technology*, Nipani, Karnataka.

Hardjono, T., & Dondeti, L. R. (2005). *Security in wireless LANs and MANs*. Artech House.

Hashim, A. T., Al-Qarrawy, S. M., & Mahdi, J. A. (2009). Design and Implementation of an Improvement of Blowfish Encryption Algorithm. IJCCCE , 9(1), 1-15.

Heys, H. M. (2002). A tutorial on linear and differential cryptanalysis. *Cryptologia*. *Taylor & Francis*, *26*(3), 189-221.

Hosseinkhani, R., & Javadi, H. H. S. (2012). Using Cipher Key to Generate Dynamic S-Box in AES Cipher System. *International Journal of Computer Science and Security (IJCSS)*, *6*(1), 19-28.

Hussain, I., Shah, T., Mahmood, H., & Afzal, M. (2010). Comparative analysis of S-Boxes based on graphical SAC. International Journal of Computer Applications. International Journal of Computer Applications, 2(5),5-8.

Isa, H., & Z'aba, M. R. (2012). Randomness analysis on LED block ciphers. *Proceedings of the Fifth International Conference on Security of Information and Networks(*pp. 60-66).ACM.

Junod, P., & Vaudenay, S. (2004). Perfect diffusion primitives for block ciphers. *Selected Areas in Cryptography* (pp. 84-99). Springer Berlin Heidelberg.

Juremi, J., Mahmod, R., & Sulaiman, S. (2012). A proposal for improving AES S-Box with rotation and key-dependent. In *Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference on* (pp. 38-42). IEEE.

Katos, V. (2005). *A randomness test for block ciphers. Applied mathematics and computation. Elsevier,162*(1), 29-35.

Kavut, S., & Yücel, M. D. (2001). On some cryptographic properties of Rijndael. *Information Assurance in Computer Networks* (pp. 300-311).Springer Berlin Heidelberg.

Kalnins, L. M. (2009). Coordinate Systems, (2009), 1–5. Retrieved from http://www.earth.ox.ac.uk/~larak/MMES/CoordinateSystems.pdf

Kazlauskas, K., & Kazlauskas, J. (2009). Key-dependent S-Box generation in AES block cipher system. *Informatics*, *20*(1), 23-34.

Keliher, L. (1997). *Substitution-permutation network cryptosystem using Key-Dependent S-Boxes*. Master thesis. Queen's university, Kingston, Ontario, Canada.

Kellerman Software, "What is The Strongest Encryption Algorithm?" July. 16, 2008 http://www.kellermansofiware.comltArticleStrongestAlgo.aspx[Accessed: June .22, 20101.

Kern, W. F. and Bland, J. R. (1948). Circular Cylinder and Right Circular Cylinder.16-17 in Solid Mensuration with Proofs, 2nd. New York: Wiley.

Kelsey, J., Schneier, B., & Wagner, D. (1997). Related-key cryptanalysis of 3-way, biham-des, cast, des-x, newdes, rc2, and tea. *Information and Communications Security*, 233-246.

Khovratovich, D., Leurent, G., & Rechberger, C. (2012). Narrow-Bicliques: cryptanalysis of full IDEA *Advances in Cryptology–EUROCRYPT 2012* (pp. 392-410): Springer.

Kiran, L. K., Abhilash, J. E. N., & Kumar, P. S. (2013). FPGA Implementation of Blowfish Cryptosystem Using VHDL. *International Journal of Engineering, 2*(1), 1-5.

Kofahi, N. A., Al-Somani, T., & Al-Zamil, K. (2004). Performance evaluation of three encryption/decryption algorithms. *Circuits and Systems, 2004 IEEE 46th Midwest Symposium on 2*(pp. 790-793). IEEE.

Krishnamurthy, G. N., & Ramaswamy, V. (2009). Performance Analysis of Blowfish and its Modified Version using Encryption quality, Key sensitivity, Histogram and Correlation coefficient analysis. *International Journal of Recent Trends in Engineering, 8*( 4),1-4.

Krishnamurthy, G. N., Ramaswamy, V., & Leela, M. G. H. (2007). Performance Enhancement of Blowfish algorithm by modifying its function. *Innovative Algorithms and Techniques in Automation, Industrial Electronics and Telecommunications* (pp. 241-244). Springer Netherlands.

Krishnamurthy, G. N., Ramaswamy, V., Leela, G. H., & Ashalatha, M. E. (2008). Blow-CAST-Fish : A New 64-bit Block Cipher, *8*(4), 282–290.

Kruppa, H., & Shahy, S. U. A. (1998). *Differential and Linear Cryptanalysis in Evaluating AES Candidate Algorithms*. ELECTRONIC REPORTING SYSTEM-ERS, National Institute of Standards and Technology.

Kumar, R. S., Pradeep, E., Naveen, K., & Gunasekaran, R. (2010). A Novel Approach for Enciphering Data of Smaller Bytes. *International Journal of Computer Theory and Engineering, 2*(4), 654-659.

Kumar, P.K., & Baskaran, K. (2010). An ASIC implementation of low power and high throughput blowfish crypto algorithm. *Microelectronics Journal*, *Elsevier*, *41*(6), 347-355.

Lai, Y.-K., & Shu, Y.-C. (1999). A novel VLSI architecture for a variable-length key, 64-bit blowfish Block cipher. *Signal Processing Systems, 1999. SiPS 99. 1999 IEEE Workshop on* (pp. 568-577). IEEE.

Lambers, J. (2009) *Three-Dimensional* Coordinate System. Lecture 17 Notes MAT 169 Fall Semester 2009-10. Retrieved from http://www.math.usm.edu/lambers/mat169/fall09/lecture17.pdf

Landge, I., Contractor, B., Patel, A., & Choudhary, R. (2012). Image encryption and decryption using blowfish algorithm. *World Journal of Science and Technology, 2*(3):151-156.

Lashkari, A. H., Danesh, M. M. S., & Samadi, B. (2009). *A survey on wireless security protocols (WEP, WPA and WPA2/802.11 i).* Paper presented at the

Computer Science and Information Technology, 2009. ICCSIT 2009. 2nd IEEE International Conference on.

Lautrup, B. (2011). *Physics of Continuous Matter: Exotic and Everyday Phenomena in the Macroscopic World*. Taylor & Francis

Limin, F., Dengguo, F., & Yongbin, Z. (2008). A fuzzy-based randomness evaluation model for block cipher. *Journal of Computer Research and Development*, *45*(12), 2095-2101.

Lin, M. C.J. & Lin, Y.L. (2000). A VLSI implementation of the blowfish encryption/decryption algorithm. In *Proceedings of the 2000 Asia and South Pacific Design Automation Conference* (pp. 1-2). ACM.

Maenhaut, M. (2010). *Coding and Cryptography Part 1*. Retrieved from www.maths.uq.edu.au/courses/MATH3302/2010/files/cryptonotes.pdf.

Mahdi, J. A. (2009). Design and Implementation of Proposed BR Encryption Algorithm. IJCCCSE, *9*(1), 1-17.

Mahmoud, E. M., Hafez, A.A.E., Elgarf, T. A., & Zekry, A.H. (2013). Dynamic AES-128 with Key-Dependent S-Box. International Journal of Engineering Research and Applications (IJERA), *3*(1), 1662–1670.

Mandal, P. C. (2012). Evaluation of performance of the Symmetric Key Algorithms: DES, 3DES, AES and Blowfish. *Journal of Global Research in Computer Science*, *3*(8), 67-70.

Manikandan, G., Manikandan, R., Rajendiran, P., Krishnan, G., & Sundarganesh, G. (2011a). An integrated block and stream cipher approach for key enhancement. *Journal of Theoretical and applied information Technology*, *28*(2), 83-87.

Manikandan, G., Kamarasan, M., Rajendiran, P., & Manikandan, R. (2011b). A hybrid approach for security enhancement by modified crypto-stegno scheme. *European Journal of Scientific Research*, *60*(2), 224-230.

Manikandan, G., Sairam, N., & Kamarasan, M. (2012b). A New Approach for Improving Data Security using Iterative Blowfish Algorithm. *Research Journal of Applied Sciences*, *4*(6), 603-607.

Manikandan, G., Rajendiran, P., Chakarapani, K., Krishnan, G., & Sundarganesh, G. (2012a). A Modified Crypto Scheme For Enhancing Data Security. *Journal of Theoretical and Applied Information Technology, 35* (2), 149-154.

Mar, P. P., & Latt, K. M. (2008). New analysis methods on strict avalanche criterion of S-Boxes. *World Academy of Science, Engineering and Technology*, 24, 150-1154.

Matsui, M. (1994). Linear cryptanalysis method for DES cipher. In *Advances in Cryptology EUROCRYPT 93*, (pp. 386-397). Springer Berlin Heidelberg.

Mattsson, J. (2006). *Stream Cipher Design*. *Master of Thesis*. Stockholm, Sweden. Citeseer.

Maximov, A. (2006). *Some Words on Cryptanalysis of Stream Ciphers*. Doctoral dissertation, Department of Information Technology Electrical and information technology , *Lund Universit.*

Meiser, G. (2007). *Efficient Implementation of Stream Ciphers on Embedded Processors.* M. Sc. Thesis, Ruhr-University Bochum, Germany.

Menezes, A., Van Oorschot, P., & Vanstone, S. (1997). *Handbook of Applied Cryptography*. CRC Press.

Meyers, R. K., & Desoky, A. H. (2008). An Implementation of the Blowfish Cryptosystem. In *Signal Processing and Information Technology, 2008. ISSPIT 2008. IEEE International Symposium on* (pp. 346-351). IEEE.

Milad, A. A., Muda, H. Z., Noh, Z. A. B. M., & Algaet, M. A. (2012). Comparative Study of Performance in Cryptography Algorithms (Blowfish and Skipjack). *Journal of Computer Science, 8* (7): 1191-1197.

MIT (2005). Review B: Coordinate Systems. Massachusetts Institute of Technology Department of Physics, 8.01.

Mohammad, F. Y., Rohiem, A. E., & Elbayoumy, A. D. (2009). A Novel S-Box of AES Algorithm Using Variable Mapping Technique. *Aerospace Sciences & Aviation Technology*(pp.1-9).

Mohan, H. S., & Red dy, A. R. (2011). Performance Analysis of AES and MARS Encryption Algorithms. *International Journal of Computer Science Issues (IJCSI), 8*(4), 363-368.

Mousa, A. (2005). Data encryption performance based on Blowfish. In *ELMAR, 2005. 47th International Symposium* (pp. 131-134). IEEE.

Mollin, R.A. (2007). *An Introduction to Cryptography*. U.S.A.: Chapman & Hall/CRC.

Mister, S., & Adams, C. (1996). Practical S-Box design. In *Workshop on Selected Areas in Cryptography, SAC* (Vol. 96, pp. 61-76).

Nadeem, A., & Javed, M. Y. (2005). A performance comparison of data encryption algorithms. *Information and communication technologies, 2005. ICICT 2005. First international conference on* (pp. 84-89). IEEE.

Naganathan, E. R., Nandakumar, V., & Dhenakaran, S. S. (2011). Identity Based Encryption Using Feistel Cipher. *European Journal of Scientific Research, 54*(4), 532–537.

Nakahara, J.J. (2008). 3D: A three-dimensional block cipher. In *Cryptology and Network Security*. (pp. 252-267). Springer Berlin Heidelberg.

Nakahara, J., J. (2007). A linear analysis of Blowfish and Khufu. In *Information Security Practice and Experience* (pp. 20-32). Springer Berlin Heidelberg.

National Institute of Standards and Technology (1999). "FIPS-46: Data Encryption Standard (DES)" *DATA Encryption Standard (DES)*. U.S.A:Federal Information Processing Standards Publication. Retrieved from http://csrc.nist .gov/publications/fips/fips46-3/fips46-3.pdf.

Nechvatal, J., Barker, E., Bassham, L., Burr, W., & Dworkin, M. (2000). Report on the development of the Advanced Encryption Standard (AES): DTIC Document.

Nguyen, P. H., Wu, H., & Wang, H. (2011). *Improving the algorithm 2 in multidimensional linear cryptanalysis.* Paper presented at the Information Security and Privacy.

Nie, T., Song, C., & Zhi, X. (2010). Performance Evaluation of DES and Blowfish Algorithms. In *Biomedical Engineering and Computer Science (ICBECS), 2010 International Conference on* (pp. 1-4). IEEE.

Nie, T., & Zhang, T. (2009). A study of DES and Blowfish encryption algorithm. In *TENCON 2009-2009 IEEE Region 10 Conference* (pp. 1-4). IEEE.

Paar, C. (2005). Applied Cryptography and Data Security. *Lecture Notes.* Retrieved from http://imperia.rz.rub.de:9085/imperia/md/content/lectures/notes.pdf

Pandey, U., Manoria, M., & Jain, J. (2012). A Novel Approach for Image Encryption by New M Box Encryption Algorithm using Block based Transformation along with Shuffle Operation. *International Journal of Computer Applications*. *Citeseer*, *42*(1), 9-15.

Patidar, V., Sud, K. K., & Pareek, N. K. (2009). A Pseudo Random Bit Generator Based on Chaotic Logistic Map and its Statistical Testing. *Informatica (Slovenia)*. *Citeseer*, *33*(4), 441-452.

Preneel, B., Biryukov, A., Oswald, E., Rompay, B. V, Granboulan, L., Dottax, E., & Dichtl, M. (2003). *NESSIE security report*. *Deliverable D20, NESSIE Consortium. Feb*.

Pub, N. F. (2001). 197. *Announcing the Advanced Encryption Standard (AES)*. Information Technology Laboratory, Processing Scientists Publication *1* 79, National Institute of Standards am1 Technology (NIST), 2001.

Ramanujam, S., & Karuppiah, M. (2011). Designing an algorithm with high avalanche effect. *International Journal of Computer Science and Network Security (IJCSNS)*, *11*(1), 106-111.

Rapeti, S. A. (2008). *NLFS: A New Non-Linear Feedback Stream Cipher*. Doctoral dissertation, Indian Institute of Technology.

Ritter, T. (1990). Substitution Cipher With Pseudo-Random Shuffling: the Dynamic Substitution Combiner. *Cryptologia*, *14*(4), 289–303. doi:10.1080/0161-119091864986

Ritter, T. (1991). TRANSPOSITION CIPHER WITH PSEUDO-RANDOM SHUFFLING : THE DYNAMIC TRANSPOSITION COMBINER. *Cryptologia*, 37–41.

Rivest, R. L., Robshaw, M., Sidney, R., & Yin, Y. L. (1998). *The RC6TM block cipher*. Paper presented at the First Advanced Encryption Standard (AES) Conference.

Rolf, O. (2005). *Contemporary Cryptography*. Artech House Computer Security Series, Boston-London.

Russ, J. C., & Russ, J. C. (2007). *Introduction to image processing and analysis*: CRC Press, Inc.

Rukhin, A., Soto, J., Nechvatal, J., Smid, M., Barker, E., Leigh, S., Levenson, M., Vangel, M. ,Banks , D. , Heckert, A., Dray, J. , Vo, S. (2010). *A statistical test suite for random and pseudorandom number generators for cryptographic application*s. National Institute of Standards and Technology Special Publication. Report number: 800-22.

Sha’ameri, A. Z. (2006*). Secured Hf Image Transmission System*. Master thesis. Universiti Teknologi Malaysia.

Schneier, B. (1996*). Applied cryptography. Protocols, Algorithms, and Source Code in C*. John Wiley & Sons, Inc.

Schneier, B. (1994). Description of a new variable-length key, 64-bit block cipher (Blowfish). In *Fast Software Encryption* (pp. 191-204). Springer Berlin Heidelberg.

Schneier, B., Kelsey, J., Whiting, D., Wagner, D., Hall, C., & Ferguson, N. (1998). Twofish: A 128-bit block cipher. *NIST AES Proposal, 15*.

Shannon, C. E. (1949). Communication theory of secrecy systems. *Bell system technical journal*, *28*(4), 656-715.

Schmidt, D. (2006). Kaweichel, an Extension of Blowfish for 64-Bit Architectures. *International Association for Cryptologic Research*, 1-8.

Sindhuja, A., Logeshwari, R., & Sikamani, K.T. (2010). A secure PMS based on Fingerprint Authentication and Blowfish cryptographic algorithm. In *Signal and Image Processing (ICSIP), 2010 International Conference on* (pp. 424-429). IEEE.

Singh, G., Singla, A. K., & Sandha, K. S. (2011). Performance Evaluation of Symmetric Cryptography Algorithms. *IJCSNS International Journal of Computer Science and Network Security*, *8*(12), 280-286.

Soto, J. (1999a). Statistical testing of random number generators. *Proceedings of the 22nd National Information Systems Security Conference*(pp.1-12). NIST Gaithersburg, MD.

Soto, J. (1999b). Randomness testing of the AES candidate algorithms. *NIST. Available via csrc. nist. gov*. Citeseer.

Soto, J., & Bassham, L. (2000). *Randomness testing of the advanced encryption standard finalist candidates*. DTIC Document.

Stallings, W. (2005). *Cryptography and Network Security*: Principles and Practices,Prentice Hall. *Inc New Jersey*.

Stamp, M. (2006).*Information Security: Principles and Practice*. John Wiley& Sons.

Stoianov, N. (2011). One Approach of Using Key-Dependent S-BOXes in AES. *In Multimedia Communications, Services and Security* (pp. 317-323). Springer Berlin Heidelberg.

Sulaiman, S., Muda, Z., & Juremi, J. (2012a). The new approach of Rijndael key schedule. In *Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference on* (pp. 23-27). IEEE.

Sulaiman, S., Muda, Z., Juremi, J., Mahmod, R., & Yasin, S.M. (2012b). A New ShiftColumn Transformation : An Enhancement of Rijndael Key Scheduling. *International Journal of Cyber-Security and Digital Forensics (IJCSDF), 1*(3), 160–166.

Sulak, F., Doganaksoy, A., Ege, B., & Koak, O. (2010). Evaluation of randomness test results for short sequences. In *Sequences and Their Applications–SETA 2010* (pp. 309-319). Springer Berlin Heidelberg.

Sulong, M. R. (2008). *Key Transformation Approach for Rijndael Security*.Master thesis. Universiti Putra Malaysia.

Suri, P R, & Deora, S. S. (2010). A Cipher based on 3D Array Block Rotation. *IJCSNS International Journal of Computer Science and Network Security, 10*(2), 186-191.

Suri, Pushpa R, & Deora, S. S. (2011). 3D array block rotation cipher: An improvement using lateral shift. *Global Journal of Computer Science and Technology*, *11*(19), 1-8.

Tamimi, A. Al. (2008). Performance analysis of data encryption algorithms. *Retrieved from* http://www.cse.wustl.edu/~jain/cse567-06/ftp/encryptionperf/index.html

Thakur, J., & Kumar, N. (2011). DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis. *International Journal of Emerging Technology and Advanced Engineering 1*(2),6-12.

Tilborg, H. C. A. van, & Jajodia, S. (2005). *Encyclopedia of Cryptography and Security*. (H. C. A. van Tilborg & S. Jajodia, Eds.). New York, USA: Springer. doi:10.1007/0-387-23483-7

Vaidhyanathan , V., Manikandan G., & Krishnan G. (2010). A Novel Approach to the Performance and Security Enhancement Using Blowfish Algorithm. *International Journal of advance Research in Computer Science, 1*(4), 451-454.

Vaudenay, S. (1995). On the weak keys of Blowfish. In *Fast Software Encryption* (pp. 27-32). Springer Berlin Heidelberg.

Vergili, I., & Yücel l, M. D. (2001). Avalanche and Bit Independence Properties for the Ensembles of Randomly Chosen S-Boxes. *Turk J Elec Engin*, *9*(2), 137-145.

Vergili, I., & Yücel, M. D. (2000) On Satisfaction of Some Security Criteria for Randomly Chosen S-Boxes. In *Proc. 20th Biennial Symp. on Communications, Kingston* (pp. 64-68).

Verma, O. P., Agarwal, R., Dafouti, D., & Tyagi, S. (2011). Peformance analysis of data encryption algorithms. *Electronics Computer Technology (ICECT), 2011 3rd International Conference on* (Vol. 5, pp. 399-403). IEEE.

Wang, Z., Graham, J., Ajam, N., & Jiang, H. (2011). Design and optimization of hybrid MD5-blowfish encryption on GPUs. *Proceedings of 2011 International Conference on Parallel and Distributed Processing Techniques and Applications (* pp.18-21). Las Vegas, Nevada, USA.

Webster, A. F., & Tavares, S. E. (1986). On the design of S-Boxes. In *Advances in Cryptology—CRYPTO'85 Proceedings* (pp. 523-534). Springer Berlin Heidelberg.

Wrede, R., & Spiegel, M. R. (2002). *Advanced, Theory and Problems of Advanced Calculus*. U.S.A.: McGraw-Hill.

Wu, Y., & Wong, S. (2004). Design Challenges in Security Processing. *15th Annual Workshop on Circuits, Systems and Signal Processing* (pp. 189-194).

Wu, H. (2004, January). A new stream cipher HC-256. In *Fast Software Encryption* (pp. 226-244). Springer Berlin Heidelberg

Zhang, R., & Chen, L. (2008). A block cipher using key-dependent S-Box and P-Boxes. *Industrial Electronics, 2008. ISIE 2008. IEEE International Symposium on* (pp. 1463-1468). IEEE.

Zhou, Q., Liao, X., Wong, K., Hu, Y., & Xiao, D. (2009). True random number generator based on mouse movement and chaotic hash function. *information sciences*. Elsevier, *179*(19), 3442-3450.

Zwillinger, D. (2003). CRC Standard Mathematical Tables and Formulae. Boca Raton, FL: CRC Press.

Zhang, Y. P., Sun, J., & Zhang, X. (2004). A stream cipher algorithm based on conventional encryption techniques. Paper presented at the Canadian Conference on Electrical and Computer Engineering, Canada.