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. Pembuatan 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 melibut pengukur 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 ia 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

Permission to Use ......................................................................................... i
Abstrak ......................................................................................................... Error! Bookmark not defined.
Abstract ...................................................................................................... Error! Bookmark not defined.
Acknowledgement ...................................................................................... iv
Table of Contents ......................................................................................... v
List of Tables ............................................................................................... x
List of Figures .............................................................................................. xii
List of Appendices ....................................................................................... xv
List of Publications ...................................................................................... xvi
List of Abbreviations ............................................................................... xviii

## CHAPTER ONE INTRUDUCTION ......................................................................... 1
1.1 Background ............................................................................................ 1
1.2 Problem Statement ............................................................................... 3
1.3 Research Questions .............................................................................. 7
1.4 Research Objectives ............................................................................ 7
1.4 Scope of Research .............................................................................. 8
1.5 Contribution of the Study ................................................................. 8
1.6 Organization of the Thesis ................................................................. 9

## CHAPTER TWO LITERATURE REVIEW ................................................................. 11
2.1 Basic Concepts of Cryptography ......................................................... 11
  2.1.1 Mode of Operation ........................................................................ 12
    2.1.1.1 Electronic Codebook (ECB) Mode .................................... 13
    2.1.1.2 Cipher Block Chaining (CBC) Mode ............................ 14
  2.1.2 Cryptographic Security Requirements ............................................ 16
    2.1.2.1 Permutation Box (P-Box) ........................................... 17
    2.1.2.2 Substitution Box (S-Box) ........................................... 18
    2.1.2.3 Dynamic P-Box and Dynamic S-Box .......................... 20
2.2 Basic Concepts of Coordinate Systems and Transformations .......... 22
  2.2.1 Coordinate Systems .................................................................... 22
    2.2.1.1 Cartesian Coordinate System .................................... 24
    2.2.1.2 Spherical Coordinate System ................................. 25
2.2.1.3 Cylinder Coordinate System ................................................. 26
2.2.2 Coordinate Transformations .................................................. 29
  2.2.2.1 Transformation of Cartesian coordinate system ................. 30
  2.2.2.2 Transformation of Polar Coordinates by a Rotation .......... 31
  2.2.2.3 Transformation of Cylindrical Coordinate System .......... 32
2.2.3 Relations among Coordinate Systems ..................................... 32

2.3 Past Related Works .................................................................. 33
  2.3.1 Pre-eSTREAM Cryptography Algorithms ............................ 33
  2.3.2 Pre-AES Cryptography Algorithms ..................................... 39
  2.3.3 Blowfish Algorithm .............................................................. 47
    2.3.3.1 Related Works on BA .................................................. 53
      2.3.3.1.1 Security Enhancement ......................................... 53
      2.3.3.1.2 Performance Enhancement ................................. 55
  2.3.4 3D Block Cipher .................................................................. 58
  2.3.5 Dynamic S-Box .................................................................. 59
  2.3.6 Secret Key Generation ......................................................... 62
  2.3.7 Dynamic P-Box .................................................................. 63
  2.3.8 Evaluation of Block Cipher .................................................. 65
    2.3.8.1 Randomness Test .......................................................... 65
      2.3.8.1.1 NIST Framework .................................................. 68
      2.3.8.1.2 Test Package ......................................................... 69
    2.3.8.2 Correlation Coefficient .................................................. 70
    2.3.8.3 Security of S-Box ......................................................... 71
      2.3.8.3.1 Avalanche Criterion .............................................. 73
      2.3.8.3.2 Strict Avalanche criterion .................................... 76
      2.3.8.3.3 Bit Independence Criterion .................................. 78
    2.3.8.4 Cryptanalysis ............................................................... 79
      2.3.8.4.1 Linear Cryptanalysis ............................................ 80
      2.3.8.4.2 Differential Cryptanalysis .................................... 81
    2.3.8.5 Computational Efficiency .......................................... 82

2.4 Summary .................................................................................. 83
CHAPTER THREE  RESEARCH METHODOLOGY .......................84
3.1 Introduction .................................................................................................................. 84
3.2 Phase 1 RAF Design ....................................................................................................... 85
  3.2.1 Dynamic 3D S-Box .................................................................................................. 85
    3.2.1.1 Generation of Random SKs .............................................................................. 90
    3.2.1.2 Define Transformations of the Right Cylinder ............................................... 92
    3.2.1.3 Byte Permutation .............................................................................................. 96
      3.2.1.3.1 Byte Relocation ......................................................................................... 96
      3.2.1.3.2 Byte Transformation ............................................................................... 100
    3.2.2 Dynamic P-Box ................................................................................................. 102
    3.2.3 Designing a New F-Function ............................................................................... 103
    3.2.4 Comparison the basic information between BA and RAF ............................... 107
3.3 Phase 2 RAF Implementation ....................................................................................... 108
  3.3.1 Key Expansion ........................................................................................................ 108
  3.3.2 Perform Data Encryption and Data Decryption ..................................................... 108
3.4 Phase 3 RAF Verification ............................................................................................. 111
  3.4.1 Stage 1 Verification of 3D S-Box ........................................................................... 111
  3.4.2 Stage 2 Verification of RAF Output ....................................................................... 114
    3.4.2.1 Part 1 Evaluation of RAF Output Using NIST Statistical Tests ..................... 114
    3.4.2.2 Part 2 Evaluation of RAF Output Using Avalanche Text and Correlation Coefficient ........................................... 120
    3.4.2.3 Part 3 Evaluation of RAF Resistance to Cryptanalysis ................................. 121
    3.4.2.4 Part 4 Evaluation of Computational Efficiency of RAF ............................... 121
  3.4.3 Stage 3 Comparison of RAF with other cryptographic algorithms .................. 122
3.5 Summary ...................................................................................................................... 122

CHAPTER FOUR  RESULTS ...............................................................................................123
4.1 Introduction .................................................................................................................. 123
4.2 Phase 1 RAF Design .................................................................................................... 123
  4.2.1 Dynamic 3D S-Box ............................................................................................. 123
    4.2.1.1 Random Secret Keys .................................................................................... 123
    4.2.1.2 Algorithms of Byte Relocation and Byte Transformation .......................... 124
  4.2.2 Dynamic P-Box ................................................................................................. 127
4.2.1 Algorithm of Dynamic P-Box .............................................. 127
4.2.2 Dynamic P-Box Values .................................................. 128
4.2.3 Cylindrical Coordinate System with Dynamic Permutation Box Function
........................................................................................................ 128
4.3 Phase 2 RAF Implementation .................................................. 138
  4.3.1 Key Expansion ............................................................ 138
  4.3.2 Data Encryption and Data Decryption ................................. 139
4.3 Summary ................................................................................... 140

CHAPTER FIVE EXPERIMENTAL RESULTS OF DYNAMIC 3D S-BOX.141
5.1 Introduction ............................................................................... 141
5.2 Results of Dynamic 3D S-Box Evaluation with 3 Criteria ............... 141
  5.2.1 AVAL Empirical Results .................................................. 141
  5.2.2 Empirical Results of SAC .............................................. 146
  5.2.3 Empirical Results of BIC .................................................. 150
5.3 Results of Correlation Coefficient on dynamic 3D S-Box in RAF ...... 154
  5.3.1 Empirical Results of Uncorrelated Random Eks .................... 154
  5.3.2 Empirical Results of Correlated Eks .................................. 157
5.4 Summary ................................................................................... 161

CHAPTER SIX EXPERIMENTAL RESULTS OF RAF .................. 162
6.1 Introduction ............................................................................... 162
6.2 Results of RAF Outputs Using NIST ........................................ 162
  6.2.1 Empirical Results on Cipher Block Chaining Mode ............... 162
  6.2.2 Empirical Results on Random Plaintext/Random 128-bit keys .... 165
  6.2.3 Empirical Results on Image Files ...................................... 167
  6.2.4 Empirical Results of Text Files ........................................ 171
  6.2.5 Empirical Results of Video Files ...................................... 173
6.3 Results of RAF Output Using Avalanche Text and Correlation Coefficient .... 176
  6.3.1 Empirical Results on Avalanche Text .................................. 176
  6.3.2 Empirical Results and Analysis on Correlation Coefficient ...... 190
6.4 Cryptanalysis ........................................................................... 193
  6.4.1 Differential and Linear Attacks ........................................ 193
6.4.2 Short Attack .................................................................................. 194
6.5 Computation Efficiency .................................................................... 195
  6.5.1 RAF .......................................................................................... 195
  6.5.2 Blowfish Algorithm (BA) ............................................................... 197
6.6 Results of Comparison on RAF with other Cryptographic Algorithms .. 198
6.7 Summary .......................................................................................... 204

CHAPTER SEVEN CONCLUSION .......................................................... 205
7.1 General Discussion .......................................................................... 205
7.2 Research achievement ..................................................................... 206
7.3 Contributions .................................................................................. 207
7.4 Limitation ....................................................................................... 210
7.5 Recommendations for Future Work ............................................... 210

REFERENCES ....................................................................................... 211
List of Tables

Table 2.1 Comparison the basic information of the most popular block cipher algorithms

Table 2.2 Comparison made between previous studies on S-Box in BA

Table 2.3 Comparisons of Pervious Studies on BA

Table 2.4 Comparison of Speeds of the Popular Algorithms

Table 2.5 NIST statistical test

Table 2.6 Minimum requirements of NIST statistical test

Table 2.7 Evaluation Procedure for a Single Binary Sequence

Table 2.8 Class of the algorithms and number of operations

Table 3.1 Five Sets of SKs

Table 3.2 Eight Transformations of the Right Cylinder

Table 5.1 $k_{AVAL}$ (i) values for the S-boxes (first random 128-bit Ek)

Table 5.2 $\epsilon_A$, Max, and Min values of $k_{AVAL}$ (ten random 128-bit Eks)

Table 5.3 $\epsilon_A$, Max, and Min values of $k_{AVAL}$ (Low entropy ones Ek)

Table 5.4 $\epsilon_A$, Max, and Min values of $k_{AVAL}$ (Low entropy zeroes Ek)

Table 5.5 $k_{SAC}$ (i, j) with random Ek of the first S-box in BA

Table 5.6 SAC of dynamic 3D S-Box in RAF

Table 5.7 $\epsilon_S$, max, and min of $k_{SAC}$ with random 128-bit Eks

Table 5.8 $\epsilon_S$, Max, and Min values of $k_{SAC}$ with Low entropy ones Ek

Table 5.9 $\epsilon_S$, Max, and Min values of $k_{SAC}$ with Low entropy zeroes Ek

Table 5.10 BIC values with random 128-bit Eks

Table 5.11 BIC values with Low entropy ones Ek

Table 5.12 BIC values with Low entropy zeroes Ek

Table 5.13 $\epsilon_{AVAL}$, $\epsilon_{SAC}$, and $\epsilon_{BIC}$ values

Table 5.14 Correlation Coefficient of 3D S-boxes (Random plaintext & uncorrelated Eks)

Table 5.15 Correlation Coefficient of dynamic 3D S-Boxes (Low entropy zeroes & uncorrelated Eks)

Table 5.16 Correlation Coefficient of dynamic 3D S-Boxes (Low entropy ones & uncorrelated Eks)

Table 5.17 Correlation Coefficient of dynamic 3D S-Boxes (Random plaintext & correlated Eks)

Table 5.18 Correlation Coefficient of dynamic 3D S-Boxes (Low entropy zeroes & correlated Eks)
Table 5.19 Correlation Coefficient of dynamic 3D S-Boxes (Low entropy ones & correlated Eks) ................................................................................................................................................. 160
Table 6.1 Avalanche text for both algorithms in the first round .......................................................................................................................... 177
Table 6.2 Avalanche text for both algorithms in the second round ................................................................................................................. 180
Table 6.3 Avalanche text for both algorithms in the third round ..................................................................................................................... 183
Table 6.4 Avalanche text for both algorithms in the ciphertext ....................................................................................................................... 186
Table 6.5 Correlation Coefficient between plaintext and ciphertext in both algorithms .................................................................................. 192
Table 6.6 Summary of the Computation Efficiency of RAF and BA .................................................................................................................. 198
Table 6.7 Comparison Randomness of RAF with finalist of AES .................................................................................................................... 204
## List of Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>ECB mode</td>
<td>14</td>
</tr>
<tr>
<td>2.2</td>
<td>CBC mode</td>
<td>16</td>
</tr>
<tr>
<td>2.3(a)</td>
<td>Cartesian coordinate system for xy-plane</td>
<td>25</td>
</tr>
<tr>
<td>2.3(b)</td>
<td>Cartesian coordinate system for xyz-space</td>
<td>25</td>
</tr>
<tr>
<td>2.4</td>
<td>Spherical coordinate system</td>
<td>26</td>
</tr>
<tr>
<td>2.5(a)</td>
<td>Right Cylinder</td>
<td>27</td>
</tr>
<tr>
<td>2.5(b)</td>
<td>Oblique Cylinder</td>
<td>27</td>
</tr>
<tr>
<td>2.6</td>
<td>Cylindrical Coordinate System</td>
<td>28</td>
</tr>
<tr>
<td>2.7</td>
<td>Level surfaces for the coordinate ρ</td>
<td>28</td>
</tr>
<tr>
<td>2.8</td>
<td>Level surfaces for the angle coordinate</td>
<td>29</td>
</tr>
<tr>
<td>2.9</td>
<td>Change in coordinates by a rotation</td>
<td>31</td>
</tr>
<tr>
<td>2.10</td>
<td>Relationship among the three coordinate systems</td>
<td>33</td>
</tr>
<tr>
<td>2.11</td>
<td>Stream Cipher</td>
<td>34</td>
</tr>
<tr>
<td>2.12</td>
<td>Encryption process in BA</td>
<td>50</td>
</tr>
<tr>
<td>2.13</td>
<td>F-Function architecture</td>
<td>51</td>
</tr>
<tr>
<td>3.1</td>
<td>Overview of the research process</td>
<td>84</td>
</tr>
<tr>
<td>3.2</td>
<td>Right cylinder</td>
<td>86</td>
</tr>
<tr>
<td>3.3</td>
<td>Cross-Section of the right cylinder</td>
<td>87</td>
</tr>
<tr>
<td>3.4</td>
<td>Representation of the right cylinder in 3D array</td>
<td>88</td>
</tr>
<tr>
<td>3.5</td>
<td>(a-d) Quarters in the first section with Byte Relocation for (a) with D₀, (b) with D₁, (c) with D₂, and (d) with D₃</td>
<td>98</td>
</tr>
<tr>
<td>3.6</td>
<td>D₀ process for the first section (a before D₀ process, b after D₀ process)</td>
<td>99</td>
</tr>
<tr>
<td>3.7</td>
<td>Rotation of a circle (ϕ₀ = π/4)</td>
<td>100</td>
</tr>
<tr>
<td>3.8</td>
<td>Rotation of the first section (ϕ₀ = π/4)</td>
<td>101</td>
</tr>
<tr>
<td>3.9</td>
<td>Translation of the first section (ρ₀ = 2)</td>
<td>101</td>
</tr>
<tr>
<td>3.10</td>
<td>Flowchart of the dynamic P-Box</td>
<td>102</td>
</tr>
<tr>
<td>3.11</td>
<td>F-Function (CCSDPB)</td>
<td>104</td>
</tr>
<tr>
<td>3.12</td>
<td>Flowchart of F-Function (CCSDPB)</td>
<td>105</td>
</tr>
<tr>
<td>3.13</td>
<td>Data Encryption RAF</td>
<td>109</td>
</tr>
<tr>
<td>3.14</td>
<td>Data decryption RAF Architecture</td>
<td>110</td>
</tr>
<tr>
<td>3.15</td>
<td>3D S-Box verification flow</td>
<td>112</td>
</tr>
<tr>
<td>3.16</td>
<td>Flow analysis of correlation coefficient of 3D S-Box in RAF</td>
<td>113</td>
</tr>
<tr>
<td>3.17</td>
<td>NIST experimental flow</td>
<td>120</td>
</tr>
</tbody>
</table>
Figure 3.19. Experimental flow on avalanche text ......................................................... 121
Figure 4.1. Random secret keys in round 0 ........................................................................ 123
Input: dynamic 3D S-Box from key expansion part .......................................................... 125
Figure 4.2. Dynamic 3D S-Box from key expansion part .................................................... 125
Figure 4.3. Dynamic 3D S-Box after BR (D0) in round 0 .................................................... 125
Figure 4.4. Dynamic 3D S-Box from BT (T8) in round 0 .................................................... 126
Figure 4.5. Dynamic 3D S-Box from BT (T4) in round 0 .................................................... 126
Figure 4.6. Dynamic 3D S-Box from BT (T6) in round 0 .................................................... 127
Figure 4.7. Dynamic P-Box in round 0 ................................................................................. 128
Figure 4.8. Output of CCSDPB Function and Ciphertext in round 0 ............................... 128
Figure 4.9. Dynamic 3D S-BOX of after apply Relocate BR (D1) in round 1 ............... 129
Figure 4.10. Random secret keys in round 1 ............................................................... 129
Figure 4.11. Dynamic 3D S-Box from BT (T8) in round 1 ................................................ 130
Figure 4.12. Dynamic 3D S-Box from BT (T4) in round 1 ................................................ 130
Figure 4.13. Dynamic 3D S-Box from BT (T6) in round 1 ................................................ 131
Figure 4.14. Dynamic P-Box in round 1 ............................................................... 131
Figure 4.15. Output of CCSDPB function and ciphertext in round 1 ........................... 131
Figure 4.16. Dynamic 3D S-Box of after apply Relocate BR (D2) in round 2 ............. 132
Figure 4.17. Random secret keys in round 2 ............................................................... 132
Figure 4.18. Dynamic 3D S-Box from BT (T8) in round 2 ................................................ 133
Figure 4.19. Dynamic 3D S-Box from BT (T4) in round 2 ................................................ 133
Figure 4.20. Dynamic 3D S-Box from BT (T6) in round 2 ................................................ 134
Figure 4.21. Dynamic P-Box in round 2 ............................................................... 134
Figure 4.22. Dynamic 3D S-Box of after apply Relocate BR (D3) in round 3 ............. 135
Figure 4.23. Random secret keys in round 3 ............................................................... 135
Figure 4.24. Dynamic 3D S-Box from BT (T4) in round 3 ................................................ 136
Figure 4.25. Dynamic 3D S-Box from BT (T6) in round 3 ................................................ 137
Figure 4.26. Dynamic P-Box in round 3 ............................................................... 137
Figure 4.27. Output of CCSDPB function and ciphertext in round 3 ........................... 137
Figure 4.28. Output of key expansion part ................................................................. 139
Figure 4.29. Data encryption and data decryption ......................................................... 140
Figure 6.1. Results of Cipher Block Chaining Mode for Round 2 in BA ...................... 163
Figure 6.2. Results of Cipher Block Chaining Mode for Round 4 in BA ...................... 163
Figure 6.3. Results of Cipher Block Chaining Mode for Round 2 in RAF .................. 164
Figure 6.4. Results of Cipher Block Chaining Mode for Round 4 in RAF .................. 164
Figure 6.5. Results of Random Plaintext/Random128-bit keys for Round 2 in BA .......... 165
Figure 6.6. Results of Random Plaintext/Random128-bit keys for Round 4 in BA .......... 166
Figure 6.7. Results of Random Plaintext/Random128-bit keys for Round 2 in RAF......... 166
Figure 6.8. Results of Random Plaintext/Random128-bit keys for round 4 in RAF ........ 167
Figure 6.9. Results of image files for Round 2 in BA............................................ 168
Figure 6.10. Results of image files for Round 4 in BA............................................ 168
Figure 6.11. Results of image files for Round 2 in RAF............................................ 169
Figure 6.12. Results of image files for Round 4 in RAF............................................ 169
Figure 6.13. Results of text files for Round 2 in BA............................................... 171
Figure 6.14. Results of text files for Round 4 in BA............................................... 171
Figure 6.15. Results of text files for Round 2 in RAF............................................. 172
Figure 6.16. Results of text files for Round 4 in RAF............................................. 172
Figure 6.17. Results of video files for Round 2 in BA............................................. 174
Figure 6.18. Results of video files for Round 4 in BA............................................. 174
Figure 6.19. Results of video files for Round 2 in RAF.......................................... 175
Figure 6.20. Results of video files for Round 4 in RAF.......................................... 175
Figure 6.21. Results of the avalanche text of both algorithms for the first round......... 189
Figure 6.22. Results of the avalanche text of both algorithms for the second round .... 189
Figure 6.23. Results of the avalanche text of both algorithms for the third round ....... 189
Figure 6.24. Results of the avalanche text of both algorithms for the ciphertext ......... 190
Figure 6.25. Results of correlation of both algorithms............................................. 191
Figure 6.26. Results of Low Density Plaintext for Round 1 in RAF ......................... 199
Figure 6.27. Results of Low Density Plaintext for Round 2 in RAF ......................... 199
Figure 6.28. Results of Low Density Plaintext for Round 3 in RAF ......................... 200
Figure 6.29. Results of Low Density Plaintext for Round 4 in RAF ......................... 200
Figure 6.30. Results of Low Density Plaintext for Round 5 in RAF ......................... 201
Figure 6.31. Results of Low Density Plaintext for Round 6 in RAF ......................... 201
Figure 6.32. Results of Low Density Plaintext for Round 7 in RAF ......................... 202
Figure 6.33. Results of Low Density Plaintext for Round 8 in RAF ......................... 202
Figure 6.34. Results of Low Density Plaintext for Round 9 in RAF ......................... 203
Figure 6.35. Results of Low Density Plaintext for Round 10 in RAF ....................... 203
List of Appendices

Appendix A NIST STATISTICAL TESTS.............................................................225
Appendix B LAST SIX ROUNDS OF RAF .........................................................228
Appendix C RESULTS OF NIST STATISTICAL TESTS .................................240
Appendix D COMPUTION EFFICIENCY OF RAF AND BA...............................263
List of Publications


# List of Abbreviations

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

INTRODUCTION

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
The contents of the thesis is for internal user only
REFERENCES


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


211


215


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


