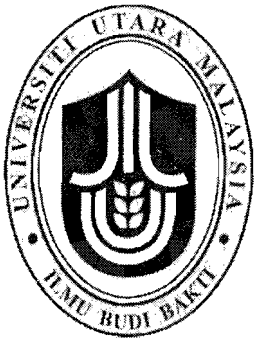
NEW CRYPTOGRAPHIC ALGORITHMS FOR ENHANCING SECURITY OF VOICE DATA

OBAIDA MOHAMMAD AWAD AL-HAZAIMEH

Universiti Utara Malaysia

UUM

2010



NEW CRYPTOGRAPHIC ALGORITHMS FOR ENHANCING SECURITY OF VOICE DATA

OBAIDA MOHAMMAD AWAD AL-HAZAIMEH

Universiti Utara Malaysia

UUM

2010

NEW CRYPTOGRAPHIC ALGORITHMS FOR ENHANCING SECURITY OF VOICE DATA

A Thesis submitted to the College of Arts and Sciences in full fulfillment of the requirements for the degree of Doctor of Philosophy

Universiti Utara Malaysia

by:

Obaida Mohammad Awad Al-Hazaimeh

PERMISSION TO USE

In presenting this thesis in partial fulfillment of the requirements for a postgraduate degree from University Utara Malaysia, I agree that the University Library may make it freely available for inspection. I further agree that permission for copying of this thesis in any manner, in whole or in part, for scholarly purposes may be granted by my supervisors in their absence, by the Dean of the Research and Graduate Studies. 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 University 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 Research and Graduate Studies

College of Arts and Sciences

Universiti Utara Malaysia

06010 UUM Sintok

Kedah Darul Aman.

NEW CRYPTOGRAPHIC ALGORITHMS FOR ENHANCING SECURITY OF VOICE DATA

ABSTRACT

A real-time application Voice over Internet Protocol (VoIP) is the technology that enables voice packets transmission over internet protocol (IP). Security is of concern whenever open networks are to be used. In general, the real-time applications suffer from packet latency and loss due to the nature of IP network. Cryptographic systems may be used to achieve VoIP security, but their impact on the Quality of Services (QoS) should be minimized. Most of the known encryption algorithms are computationally expensive resulting in a significant amount of time added to packet delay. VoIP is usually used by public users resulting in a key exchange problem and a trusted intermediate authority normally takes this responsibility. In this research, VoIP security was enhanced via a proposed cryptographic system. The proposed solution consists of a simple, but strong encryption/decryption algorithm as well as an embedded method to exchange the keys between the users. In this research, a new keys is generated in a random fashion and then used to encrypt each new voice packet to strengthen the security level. Key exchange is carried out by inserting the key with the ciphered voice packet that depends on the table of the key positions at the sender and receiver sides, and the target receiver is the only one who is able to extract the key. The encryption process in this research is divided into three main stages: key generation, encryption process, and key insertion process. The decryption process on the other hand is divided into two main stages: key extraction process, and decryption process. The proposed solution was implemented and tested and the results showed that the required time for the security processes is minimized compared to some known algorithms such as AES_Rijndael algorithm. Furthermore, the analysis has proved that the security level has a direct relationship to the key length and the voice packet size in that large packet size requires more processing time. Finally, the implementation result in this research shows the average time needed to encrypt and decrypt a voice packet size using a proposed algorithm with the long key of 1024-bits is much smaller than AES_Rijndael algorithm with a short key length of 128-bits.

ABSTRACT

A real-time application Voice over Internet Protocol (VoIP) is the technology that enables voice packets transmission over internet protocol (IP). Security is of concern whenever open networks are to be used. In general, the real-time applications suffer from packet latency and loss due to the nature of IP network. Cryptographic systems may be used to achieve VoIP security, but their impact on the Quality of Services (QoS) should be minimized. Most of the known encryption algorithms are computationally expensive resulting in a significant amount of time added to packet delay. VoIP is usually used by public users resulting in a key exchange problem and a trusted intermediate authority normally takes this responsibility. In this research, VoIP security was enhanced via a proposed cryptographic system. The proposed solution consists of a simple, but strong encryption/decryption algorithm as well as an embedded method to exchange the keys between the users. In this research, a new keys is generated in a random fashion and then used to encrypt each new voice packet to strengthen the security level. Key exchange is carried out by inserting the key with the ciphered voice packet that depends on the table of the key positions at the sender and receiver sides, and the target receiver is the only one who is able to extract the key. The encryption process in this research is divided into three main stages: key generation, encryption process, and key insertion process. The decryption process on the other hand is divided into two main stages: key extraction process, and decryption process. The proposed solution was implemented and tested and the results showed that the required time for the security processes is minimized compared to some known algorithms such as AES_Rijndael algorithm. Furthermore, the analysis has proved that the security level has a direct relationship to the key length and the voice packet size in that large packet size requires more processing time. Finally, the implementation result in this research shows the average time needed to encrypt and decrypt a voice packet size using a proposed algorithm with the long key of 1024-bits is much smaller than AES_Rijndael algorithm with a short key length of 128-bits.

ABSTRAK

Aplikasi suara masa benar (*real-time*) melalui protokol Internet (VoIP) ialah teknologi yang membolehkan paket suara ditransmisi melalui Protocol Internet (IP). Keselamatan adalah perkara yang perlu dititikberatkan apabila jaringan terbuka digunakan. Secara umumnya, aplikasi masa benar (*real-time*) mempunyai kelemahan disebabkan oleh kependaman paket and kehilangannya yang disebabkan oleh jaringan semula jadi IP. Sistem Kriptografi yang digunakan mungkin boleh meningkatkan keselamatan VoIP, tetapi kesannya terhadap Kualiti Servis (QoS) juga perlu dikurangkan. Kebanyakan algoritma enkripsi yang diketahui mempunyai pengiraan yang keterlaluan dan ini mengakibatkan masa penangguhan paket bertambah. VoIP yang biasanya digunakan oleh pengguna awam menyebabkan masalah pertukaran kekunci and biasanya orang pertengahan yang dipercayai akan mengambil alih tanggungjawab ini. Dalam penyelidikan ini, keselamatan VoIP dipertingkatkan dengan menggunakan sistem kriptografi yang disarankan. Saranan penyelesaian ini mudah, tetapi ia mempunyai algoritma enkripsi/dekripsi yang kukuh dan mengandungi kaedah pertukaran kekunci di antara penguna. Dalam kajian ini, kekunci baharu dijana secara rawak dan kemudiannya digunakan untuk mengenkripsi setiap suara paket yang baharu bagi memperkukuh tahap keselamatan. Pertukaran kekunci dilakukan dengan memasukkan kekunci melalui tulisan rahsia paket suara yang bergantung pada jadual kedudukan kekunci pada pihak penghantar dan pihak penerima serta sasaran penerima adalah sesiapa yang boleh mengekstrak kekunci tersebut. Proses enkripsi dalam kajian ini dibahagikan kepada tiga peringkat utama: penjanaan kekunci, proses enkripsi dan proses memasukkan kekunci. Proses dekripsi pula dibahagikan kepada dua peringkat utama: proses mengekstrak kekunci dan proses dekripsi. Penyelesaian yang dicadangkan telah dilaksanakan dan diuji serta keputusan menunjukkan bahawa masa yang diperlukan untuk proses keselamatan telah dikurangkan berbanding algoritma yang diketahui seperti algoritma AES_Rijndael. Tambahan pula, analisis juga membuktikan bahwa tahap keselamatan mempunyai hubungan langsung dengan panjang kekunci dan saiz suara paket di mana paket saiz yang besar memerlukan masa pemprosesan yang lebih panjang. Akhir sekali, keputusan yang didapati daripada kajian ini menunjukkan purata masa yang diperlukan untuk mengenkripsi dan mengdekripsi saiz suara paket yang menggunakan algoritma yang dicadangkan, walaupun menggunakan kekunci yang panjang iaitu 1024-bit, adalah lebih pendek berbanding algoritma AES_Rijndel yang menggunakan kekunci yang pendek iaitu hanya 128-bit.

ABSTRACT

A real-time application Voice over Internet Protocol (VoIP) is the technology that enables voice packets transmission over internet protocol (IP). Security is of concern whenever open networks are to be used. In general, the real-time applications suffer from packet latency and loss due to the nature of IP network. Cryptographic systems may be used to achieve VoIP security, but their impact on the Quality of Services (QoS) should be minimized. Most of the known encryption algorithms are computationally expensive resulting in a significant amount of time added to packet delay. VoIP is usually used by public users resulting in a key exchange problem and a trusted intermediate authority normally takes this responsibility. In this research, VoIP security was enhanced via a proposed cryptographic system. The proposed solution consists of a simple, but strong encryption/decryption algorithm as well as an embedded method to exchange the keys between the users. In this research, a new keys is generated in a random fashion and then used to encrypt each new voice packet to strengthen the security level. Key exchange is carried out by inserting the key with the ciphered voice packet that depends on the table of the key positions at the sender and receiver sides, and the target receiver is the only one who is able to extract the key. The encryption process in this research is divided into three main stages: key generation, encryption process, and key insertion process. The decryption process on the other hand is divided into two main stages: key extraction process, and decryption process. The proposed solution was implemented and tested and the results showed that the required time for the security processes is minimized compared to some known algorithms such as AES_Rijndael algorithm. Furthermore, the analysis has proved that the security level has a direct relationship to the key length and the voice packet size in that large packet size requires more processing time. Finally, the implementation result in this research shows the average time needed to encrypt and decrypt a voice packet size using a proposed algorithm with the long key of 1024-bits is much smaller than AES_Rijndael algorithm with a short key length of 128-bits.

الأهداء

مهما كتبت من كلمات ومهما انتقيت من الحروف ومهما نسجت من الجمل في النهاية اهدي هذه الاطروحة الى من علمني كيف احزن دون ان أحزن من حولى، وكيف أفرح ليفرح من حولي الى من علمني ان التضحية مفتاح العطاء، الى الرجولة بذاتها وعماد البيت ، الى صاحب اجمل قطرات العرق المتصببة على الجبين ، الى البحر الذي ادخل في شخصيتي الحب ، الى الذي تعلمت من خلاله الصبر والصمود في هذه الحياة ، الى اول من علمني ابجدية الحروف فكانت اول ما نطق بها لساني الى من اخذ بيدي كي احلل تلك الرموز والمتاهات الموجودة في هذه الحياة الى .....

أبي العزيز

ابو عبيـــــــــــــــــده

الى من علمتني العطف والتسامح، الى التي تحترق لتنير لنا الطريق وتعلمنا معنى الصديق وتنتشلنا من كل ضيق وتكون لنا خير رفيق، الى.....

أمي الغالية

ام عبيـــــــــــــــــده

DEDICATION

Dedicated to one of the most Amazing Men

My father

Dedicated to a Great Mom

To my beloved brothers Abdullah, Amer, Awad, Omar and

Osman

To my beloved sister Sajedah

Especially

To my beloved brother AMER MOH'D who have encouraged

and helped me very much during my study

(عامـــــــــــــــــــــــــــر)

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABBREVIATIONS

A/D:	Analog-to-Digital
AC:	Authentication Centers
ACELP:	Algebraic Code Excited Linear Predictive
ADPCM:	Adaptive Differential Pulse Code Modulation
AES:	Advanced Encryption Standard
CA:	Certificate Authorities
CBC:	Cipher Block Chaining
CFB:	Cipher Feedback
CRHF:	Collision Resistant Hash Function
CRL:	Certificate Revocation List
CS-ACELP:	Conjugate Structure Algebraic Code Excited Linear Predictive
DA:	Destination Address
D/A:	Digital-to-Analog
Dual-C:	Dual-Core
DES:	Data Encryption Standard
DS:	Differential Service
DHCP:	Dynamic Host Configuration Protocol
DIX:	DEC, Intel, Xerox
DSP:	Digital Signal Processing
ECN:	Explicit Congestion Notification
EF:	Expedited Flow
ENT:	ENTROPY

FCS:	Frame Check Sequence
FIPS:	Federal Information Processing Standards
FTP:	File Transfer Protocol
IAB:	Internet Architecture Board
ICR:	Interface Clock Rate
IEEE:	Institute of Electrical and Electronics Engineers
IETF:	Internet Engineering Task Force
IP:	Internet Protocol
IPSec:	Internet Protocol Security
IPv4:	Internet Protocol version 4
IPv6:	Internet Protocol version 6
ISP:	Internet Service Provider
ITU:	International Telecommunication Union
ITU-T:	ITU Telecommunication Standardization Sector
LA:	Look Ahead time
LAN:	Local Area Network
LDAU:	Last Data Added Users
LFSR:	Linear Feedback Shift Register
LFI:	Link Fragmentation and Interleaving
MAC:	Message Authentication Code
MAD:	Modification Detection Code
MoS:	Mean Opinion Score
MP-MLQ:	Multi-Pulse Maximum Likelihood Quantization

ms:	millisecond
MTU:	Maximum Transmission Unit
ND:	Network Delay
NIST:	National Institute of Standards and Technology
OPSO:	Overlapping-Pairs-Sparse-Occupancy
OQSO:	Overlapping-Quadruples-Sparse-Occupancy
OSI:	Open Systems Interconnection
OWHF:	One Way Hash Function
PBX:	Private Branch eXchange
PC:	Personal Computer
PCM:	Pulse Code Modulation
PKI:	Public Key Infrastructure
PLC:	Packets Loss Concealment
PRNG:	Pseudorandom Number Generator
PSTN:	Public Switched Telephone Network
PT:	Payload Type
QD:	Queuing Delay
QoS:	Quality of Service
RA:	Registration Authority
RAM:	Random Access Memory
RAS:	(Registration, Admission, and Status) Signaling
RFC:	Request for Comments
RSA:	Rivest, Shamir, Adelman

RNG:	Random Number Generators
RTCP:	RTP Control Protocol
RTP:	Real-time Transport Protocol
RTPC:	Real-time Transport Protocol Header Compression
SA:	Source Address
SCC:	Serial Correlation Coefficient
SD:	Serialization Delay
SDK:	Software Developer's Kit
SFD:	Start of Frame Delimiter
SIP:	Session Initiation Protocol
SSRC:	Synchronization Source
S-Box:	Substitution-Box
TCP:	Transmission Control Protocol
TOS:	Type of Service
UDP:	User Datagram Protocol
URL:	Universal Resource Locator
UUM:	Universiti Utara Malaysia
VAD:	Voice Activity Detection
VoIP:	Voice over Internet Protocol
WAN:	Wide Area Network

CHAPTER ONE

INTRODUCTION

1.1 INTRODUCTION

Real-time application Voice over Internet Protocol (VoIP) refers to the technology that transfers voice data over Internet Protocol (IP) networks. It conveys real-time audio information such as human voice, in a manner that emulates traditional telephone service [1]. The VoIP technology relies on the fundamental internet architecture principle which allows any computer with an IP address to send any kind of data to any other computer with an IP address. In general, the VoIP technology only requires an Internet connection and a program on the endpoint computer capable of encoding and transmitting speech [2-3].

Among the advantages of the VoIP technology over the traditional Public Switch Telephone Network (PSTN) are lower cost, integration with other media services, portability, and bandwidth utilization. For instance, the network and service providers consider the VoIP technology as a mean of reducing the cost of offering existing voice-based services and new multimedia services. In addition, the VoIP infrastructure is viewed as an economical base in building new revenue-generating services. Most importantly, the deployment of VoIP technology is becoming widespread and forming part of a shared competitive landscape [4].

The contents of the thesis is for internal user only

REFERENCES

[1] M. Hil. and G. Zhang, "A Web Services Based Framework for Voice over IP", *Proceedings of the 30th Euromicro Conference*, vol. 10, pp. 258 – 264, 2004.

[2] S. Bellovin, M. Blaze, E. Brickell, C. Brooks, V. Cerf, W. Diffie, S. Landau, J. Peterson, and J. Treichler, "Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP", *Information Technology Association of America,* 2006. [Online]. Available at: http://www.cs.columbia.edu/~smb/papers/CALEAVOIPreport.pdf.

[3] C. Hett, N. Kuntze, and A. Schmidt, "Security and Non-Repudiation for Voice-over-IP Conversations," Diploma of Science dissertation, Fraunhofer-Institut for Sichere Informations Technologie, 2006.

[4] S. Ahuja and R. Ensor, "VoIP: What is it Good for?", *Association for Computing Machinery Queue (ACM Queue)*, vol. 2, pp. 55-58, 2004.

[5] P. Zimmerman, *An Introduction to Cryptography,* Doubleday & Company, Inc., United State of America, USA, 1999.

[6] T. Walsh and D. Kuhn, "Challenges in Securing Voice Over IP", *IEEE Security and Privacy* , vol. 3, pp. 44-49, 2005.

[7] J. Bilien, "Key Agreement for Secure Voice over IP", Master of Science Dissertation, Center for Wireless Systems and Telecommunication Systems Laboratory, Stockholm, 2003.

[8] A. Elb. and S. Shepherd, "A Comprehensive Secure VoIP Solution", *International Journal of Network Security*, vol. 5, pp. 233-240, 2007.

[9] B. Goode, "Voice over Internet Protocol (VoIP)", *Proceedings of IEEE*, vol. 90, pp. 1495-1517, 2002.

[10] J. Light and A. Bhu, "Performance Analysis of Audio Codecs over Real-Time Transmission Protocol (RTP) for Voice Services over Internet Protocol", *Proceedings of the 2nd Annual Conference on Communication Networks and Services Research*, vol. 12, pp. 351 – 356, Canada, 2004.

[11] M. Collier, "Vulnerabilities and Solutions", *International Journal of Data Communication Management*, vol. 2, pp. 1-15, 2005.

[12] J. Ransome and J. Rit., *VoIP Security: VoIP Security Best Practices*, Elsevier Digital Press, Newton, USA, 2005.

[13] V. Casola, M. Rak, A. Mazzeo, and N. Mazzoccca, "Security Design and Evaluation in a VoIP Secure Infrastructure: A Policy Based Approach", *Proceedings of the Information Technology Conference: Coding and Computing (ITCC'05)*, vol. 1, pp. 727 – 732, Las Vegas, Nevada, 2005.

[14] A. Tyagi, "VoIP Performance on Differentiated Services Enabled Network", *in the Proceedings of the 8th IEEE International Conference on Networks (ICON'00)*, vol. 10, pp. 419 – 423, Singapore, 2000.

[15] D. Greenstreet and S. Scoggins, "Building Residential VoIP Gateways", *A Tutorial Part Four: VoIP Security Implementation,* 2004, [Online]. Available at: http://www. analogzone .com/nett0913. pdf.

[16] K. Werbach, "Using VoIP to Compete," *Harvard Business Review*, vol. 83, pp. 140-147, 2005.

[17] M. Wali and M. Rehan, "Effective Coding and Performance Evaluation of the Rijndael Algorithm (AES)", *in the Proceedings of the Engineering Sciences and Technology Conference*, vol. 7, pp. 1-7, Karachi, 2005.

[18] S. Chang, "The Design of A Secure and Pervasive Multimodal Web System", *in the Proceedings of the 17th International Conference on Advanced Information Networking and Applications (AINA'05)*, vol. 2, pp. 683 – 688, Taiwan, 2005.

[19] M. Islam, N. Mia, M. Chow, and M. Matin, "Effect of Security Increment to Symmetric Data Encryption Through AES Methodology", *in the Proceedings of Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing Conference*, vol. 9, pp. 291 - 294, Phuket, 2008.

[20] R. Sever, A. Isma., Y. Tekmen, and M. Askar, "A High Speed ASIC Implementation of the Rijndael Algorithm", *in the Proceedings of the International Symposium on Circuits and Systems (ISCAS'04)*, vol.2, pp. II - 541-4, France, 2004.

[21] S.T., Sivaram.L, A.S, D. Ranjan . S, and Vaidehiv, "Reduction in Computational Complexity of a Fast Encryption Algorithm for Application in Voice Oriented System", *in the Proceedings of the IEEE-International Conference on Signal Processing, Communications and Networking*, pp. 97-101, India, 2008.

[22] P. Sherburne and C. Fitzgerald, "You Don't Know Jack About VoIP", *Association for Computing Machinery Queue (ACM Queue)*, vol. 2, pp. 30-38, 2004.

[23] P. Release, "VoIP Security and Privacy Threat Taxonomy", *VoIP Security Alliance*, 2005, [Online]. Available at: http://www.voipsa.org/Activities/VOIPSA_Threat_Taxonomy_0.1.pdf .

[24] J.-I. Guo, J.-C, Yen, H.-F. Pai, "New Voice over Internet Protocol Technique with Hierarchical Data Security Protection", *in the Proceedings of the IEE Vision, Image and Signal Processing*, vol. 149, pp. 237-243, 2002.

[25] D. Butcher, L. Xiang, and G. Jinhua, "Security Challenge and Defense in VoIP Infrastructures", *IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews,* vol. 37, pp. 1152 – 1162, 2007.

[26] L. Balliache, "Network Traffic Control Network Modeling, Voice over IP", *Practical QoS,* 2003, [Online]. Available at: http://www.opalsoft.net/qos/.

[27] W. Wang, S. Liew, and V. Li, "Solutions to Performance Problems in VoIP over A 802.11 Wireless LAN", *IEEE Transactions on Vehicular Technology*, vol. 54, pp. 366 – 384, 2005.

[28] U. Black, *Voice over IP:Prentice Hall Series in Advanced Communications Technologies*. New Jersey, USA, 2001.

[29] N. Inc, "Voice over Packet: An Assessment of Voice Performance on Packet Networks", *Nortel Networks*, 2001, [Online]. Available at: http://www.nortel.com/products/library/collateral/74007.25-09-01.pdf.

[30] N. Inc, "VoIP Bandwidth Calculation", *Newport Network,* 2005, [Online]. Available: http://kambing.ui.ac.id/onnopurbo/library/library-ref-eng/ref-eng-3/physical/voip/52-VoIP-Bandwidth.pdf.

[31] D. Kuhn, T. Walsh, and S. Fries, "Security Considerations for Voice over IP Systems", *Recommendations of the National Institute of Standards and Technology (NIST), Special Publication* 800-58, 2005, [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf.

[32] M. Grant and S. Tenissen, *Voice Quality Monitoring for VoIP Networks*, Calyptech, Australia, 2005.

[33] D. I. Cisco, "Understanding Delay in Packet Voice Networks", *Cisco*, 2006, [Online]. Available at: http://www.cisco.com/warp/public/788/voip/delay-details.html.

[34] J. Davidson and J. Peters, *Voice over IP Fundamentals: A Systematic Approach to Understanding the Basics of Voice over IP*, 2nd ed: Cisco Press, 2006.

[35] M. Hillenbrand, J. Götze, and P. Müller, "Voice over IP-Considerations for A Next Generation Architecture", *in the Proceedings of the 31st EUROMICRO Conference on Software Engineering and Advanced Applications*, vol. 12, pp. 386-393, Portugal, 2005.

[36] S. Zeadally, F. Sid, and P. Ku, "Voice over IP in Intranet and Internet Environments", *IEE Proceedings-Communications*, vol. 151, pp. 263-269, 2004.

[37] A. Markopoulou, F. Tobagi, and M. Karam, "Assessment of VoIP Quality over Internet Backbones", *in the Proceeding of IEEE INFOCOM Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies*, vol.1, pp. 150-159, New York, 2002.

[38] J. Sinclair and P. Fong, *Configuring Cisco Voice Over IP*, 2nd ed., Syngress Publishing, Inc., United State of America, 2002.

[39] G. Eriksson, B. Olin, K. Sv., and D. Turina, "Challenges of Voice-Over-IP-Over-Wireless", *Ericsson Rev. (ENGL ED)*, vol. 77, pp. 20-31, 2000.

[40] J. Perez, V. Zarate, A. Montes, and C. Garcia, "Quality of Service Analysis of IPSec VPNs for Voice and Video Traffic", *in the Proceedings of the Advanced International Conference on Internet and Web Applications and Services (AICT-ICIW'06)*, vol. 10, pp. 43-43, French Caribbean, 2006.

[41] L. Gao and J. Luo, "Performance Analysis of a P2P-Based VoIP Software", *in the Proceedings of the Advanced International Conference on Internet and Web Applications and Services (AICT-ICIW'06)*, vol. 10, pp. 11-11, French Caribbean, 2006.

[42] J. Walker, "A Handbook for Successful VoIP Deployment: Network Testing, QoS, and More ", *NetIQ Corporation* , pp. 1-13, US, 2002, [Online]. Available at: http://download.netiq.com/CMS/NetIQ_Handbook_for_Successful_VoIp_Deployment.pdf.

[43] J. Zhang, D. Yang, and Z. Quan, "Voice Quality of VoIP in Mobile Communication Systems", *in the Proceedings of the IEEE Radio and Wireless Symposium*, vol. 45, pp. 131-134, 2006.

[44] A. Nascimento, A. Passito, E. Mota, E. Nascimento, and L. Carvalho, "Can I Add A Secure VoIP Call?", *Proceedings of the International Symposium on A World of Wireless, Mobile and Multimedia Networks*, vol. 2, pp. 779-783, 2006.

[45] T. Xie and X. Qin, "Enhancing Security of Real-Time Applications on Grids through Dynamic Scheduling", *Proceedings of the Job Scheduling Strategies for Parallel Processing*, vol. 38, pp. 219-237, 2005.

[46] E. Guillen and D. Chacon, "VoIP Networks Performance Analysis with Encryption Systems", *International Journal of World Academy of Science, Engineering and Technology*, vol. 58, pp. 688-695, 2009.

[47] H. Chong and H. Matthews, "Comparative Analysis of Traditional Telephone and Voice-Over-Internet Protocol (VoIP) Systems", *in the Proceedings of the IEEE International Symposium on Electronics and the Environment*, vol. 10, pp. 106-111, USA, 2004.

[48] A. Escudero., and Ber., L, *VoIP-4D Primer Building Voice Infrastructure in Developing Regions*, Elsevier Digital Press, USA, 2006.

[49] W. Stallings, *Computer Networking with Internet Protocols and Technology*, New Jersy, USA, Pub Pearson Prentice Hall, 2004.

[50] S. Deering and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", *RFC 2460, Internet Engineering Task Force*, 1998, http://www.ietf.org/rfc/rfc2460.txt.

[51] B. Ong, "A Hybrid Mechanism for SIP Over IPv6 Macromobility and Micromobility Management Protocols", PhD dissertation, Universiti Utara Malaysia (UUM), Malaysia, 2007.

[52] O. Ghazali, "Scaleable and Smooth TCP-Friendly Receiver-Based Layered Multicast Protocol", PhD dissertation, Universiti Utara Malaysia (UUM), Malaysia, 2008.

[53] N. Sharda, "Multimedia Networks: Fundamentals and Future Directions", *Communications of the Association for Information Systems (AIS)*, vol. 1, pp. 553 - 558, 1999.

[54] M. Goncalves, *IPv6 networks*, McGraw-Hill, Inc. New York, NY, United stated of America, 2002.

[55] A. Tanenbaum, *Computer Networks,* 2nd ed., United States of America, New Jersey: Prentice Hall, 1989.

[56] C. Metz, "Internet Multimedia: Answering Basic Question", *IEEE Internet Computing*, vol. 9, pp. 51-55, 2005.

[57] R. Prasad, R. Hurni, and H. Jam, "A Scalable Distributed VoIP Conferencing using SIP", *in the Proceedings of the Eighth IEEE International Symposium on Computers and Communication (ISCC)*, pp. 608, Turkey, 2003.

[58] S. Bradner and C. Metz, "Guest Editors' Introduction: The Continuing Road Toward Internet Media", *IEEE Internet Computing*, vol. 9, pp. 19-21, 2005.

[59] M. Moh, G. Berquin, and Y. Chen, "Mobile IP Telephony: Mobility Support of SIP", *in the Proceedings of the Eighth IEEE International Conference on Computer Communications and Networks*, vol. 18, pp. 554-559, Boston, USA, 1999.

[60] J. Ros, H. Sch, G. Cam, A. Johnston, J. Pete, R. Sparks, M. Han, and E. Sch, "SIP: Session Initiation Protocol", *RFC 3261, The Internet Engineering Task Force*, 2002. http://www.ietf.org/rfc/rfc3261.txt.

[61] A. Kumar, "An Overview of Voice Over Internet Protocol (VOIP)," *Journal of Rivier College Online Academic*, vol. 2, pp. 1-13, 2006.

[62] I. Rec, "G.114 One-Way Transmission Time Series G: Transmission Systems and Media, Digital System and Network", *International Telecommunication Union (ITU-T),* 2003, [Online]. Available at: http://www.cs.columbia.edu/~andreaf/new/documents/other/T-REC-G.114-200305.pdf.

[63] R. Barbieri, D. Bruschi, and E. Rosti, "Voice Over IPsec: Analysis and Solutions", *in the Proceedings of the 18th Annual Computer Security Applications Conference*, vol. 10, pp. 261 – 270, San Diego California, 2002.

[64] T. Kostas, M. Borella, I. Sidhu, G. Schuster, J. Grabiec, and J. Mahler, "Real-Time Voice Over Packet-Switched Networks", *IEEE network*, vol. 12, pp. 18-27, 1998.

.[65] P. Mehta and S. Udani, "Overview of Voice Over IP", *University of Pennsylvania, Technical Report (MS-CIS-01-31)* 2001, [Online]. Available at: http://www.coe.montana.edu/ee/rwolff/EE548/papers/VoIP/upenn_Overview_VoIP.pdf.

[66] A. Ma, "Voice over IP (VoIP)", *Spirent Communications*, United States America: Inc, 2001.

[67] R. Mollin, *An Introduction to Cryptography (Discrete Mathematics & Its Applications Series)*, Chapman & Hall/CRC, Inc. USA, 2007.

[68] W. Stalling, *Computer Networking with Internet Protocol and Technology*. United States America, New Jersey: Pearson Prentice Hall, 2004.

[69] A. Meneze, *Elliptic Curve Public Key Cryptosystems*, Kluwer Academic Publisher Group, United States America, The Netherlands, 1993.

[70] H. Mou., P. Giorgini, and G. Manson, "Modelling Secure Multiagent Systems", *in the Proceedings of the Second International Joint Conference on Autonomous Agents and Multiagent Systems (AAMAS'03)*, pp. 859-866, Melbourne, Australia, 2003.

[71] M. Pearl, "The Codebreakers. The Story of Secret Writing", *David Kahn. Weidenfeld, Nicolson and Macmillan*, London, New York, vol. 161, pp. 35-36, 1968.

[72] H. Feistel, "Cryptographic Coding for Data Bank Privacy", *IBM Corp. T.J. Watson Res. Ctr. Rep. RC*2827, vol. 2827, Yorktown Heights, NY, 1970.

[73] A. Beut, *Cryptology: An Introduction to the Art and Science of Enciphering, Encrypting, Concealing, Hiding, and Safeguarding Described Without Any Arcane Skullduggery But Not Without Cunning Waggery for the Delectation and Instruction of the General Public*, Mathematical Association of America, Washington, D.C, 1996.

[74] D. R. Stinson, *Cryptography: Theory and Practice,* 2nd ed. Chapman & Hall/CRC, Inc., USA, 2007.

[75] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. CRC Press, 2001. [Online]. Available at: http://www.cacr.math.uwaterloo.ca/hac/.

[76] N. Daswani, C. Kern, and A. Kesavan ,*Foundations of Security: What Every Programmer Needs to Know*, Apress, United States America, NY, USA, 2007.

[77] C. Karlof, N. Sastry, and D. Wagner, "TinySec: A Link Layer Security Architecture for Wireless Sensor Networks", *in the Proceeding of 2nd International Conference on Embedded Networked Sensor Networks* , vol. 17, pp. 162-175, Baltimore, Maryland, USA, 2004.

[78] M. Robshaw, "Stream ciphers", *RSA Labratories Technical Report TR-701.* Version 2 ,1995.

[79] W. Stalling, *Cryptography and Network Security: Principles and Practice,* 4th ed. United States America, New Jersey: Pearson Prentice Hall, 2006.

[80] H. Delfs and H. Knebl, *Introduction to Cryptography: Principles and Applications Series: Information Security and Cryptography*, 2nd ed. Springer-Verlag, New York Inc, 2002.

[81] M. Bishop, *Computer Security: Art and Science*, MA: Addison-Wesley, Boston, 2003.

[82] W. Stalling, *Introduction to Cryptography: Principles and Applications*, United States America, New Jersey: Pearson Prentice Hall, 2006.

[83] R. Mollin, *Codes: The Guide to Secrecy from Ancient to Modern Time:* Taylor & Francis Group, CRC Press, NY, USA, 2005.

[84] H. Lee and S. Moon, "Parallel Stream Cipher for Secure High-Speed Communications", *Journal of Signal Processing*, vol. 82, pp. 259-265, 2002.

[85] A. Sterbenz and P. Lipp, "Performance of The AES Candidate Algorithms in Java", *in the Proceedings in the Third AES Candidate Conference, National Institute of Standards and Technology (NIST)*, New York, NY, USA, 2000, [Online]. Available at: http://www.nist.gov/aes.

[86] W. B. Diab, S. Tohme, and C. Bassil, "Critical VPN Security Analysis and New Approach For Securing VoIP Communications over VPN Networks", *in the Proceedings of the 3rd ACM Workshop on Wireless Multimedia Networking and Performance Modeling*, vol. 11, pp. 92 - 96, Chania, 2007.

[87] N. FIPS, "197: Announcing The Advanced Encryption Standard (AES)", *Information Technology Laboratory, Processing Standards Publication 179, National Institute of Standards and Technology (NIST)*, 2001.

[88] W. Diffie and M. E.Hellman, "New Directions in Cryptography", *IEEE Transactions on Information Theory*, vol. 22, pp. 644 – 654, 1976.

[89] R. L. Rivest, A. Shamir, and L. M. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", *Communications Journal of the ACM*, vol. 21, pp. 120-126, 1978.

[90] N. Challa and J. Pradhan, "Performance Analysis of Public Key Cryptographic Systems RSA and NTRU", *International Journal of Computer Science and Network Security*, vol. 7, pp. 87-96, 2007.

[91] T. Hardjono and L. Dondeti, *Computer Security Series: Security in Wireless LANs and MANs*, Artech House Publishers, 2005.

[92] J. Edney and W. Arbaugh, "Real 802.11 Security: Wi-Fi Protected Access and 802.11", *Addison Wesley Publishing Company*, 2nd ed., Pearson Education, Inc. USA, 2004.

[93] A. Elb and S. Shepherd, "Stream or Block Cipher for Securing VoIP?", *International Journal of Network Security*, vol. 5, pp. 128-133, 2007.

[94] A. Nadeem and M.Y. Javed, "A Performance Comparison of Data Encryption Algorithms", *in the Proceeding IEEE Information and Communication Technologies International Conference*, vol. 6, pp. 84-89, Chania, 2005.

[95] S. Standard, "FIPS Pub 180-1", *National Institute of Standards and Technology (NIST)* vol. 17, 1995. [Online]. Available at: http://www.itl.nist.gov/fipspubs/fip180-1.htm.

[96] B. Pre., A. Bos., and H. Dob., "The Cryptographic Hash Function RIPEMD-160", *RSA Laboratories CryptoBytes* ,vol. 22, pp. 24-28, 1997.

[97] S. Ahson and M. Ilyas, *VoIP Handbook: Applications, Technologies, Reliability, and Security*: Taylor & Francis Group, CRC Press, 2008.

[98] C. Jie, "Design Alternatives and Implementation of PKI Functionality for VoIP", Master of Science dissertation, Telecommunication Systems Laboratory, Royal Institute of Technology (KTH), Stockholm, 2006.

[99] S. Xenitellis, *The Open-Source PKI Book: A Guide to PKIs and Open-Source Implementations*, Open CA Team, 2000.

[100] R. Hunt, "PKI and Digital Certification Infrastructure", *in the Proceedings Ninth IEEE International Conference on Networks*, vol. 4, pp. 234 – 239, Bangkok, Thailand, 2001.

[101] R. Perlman, "An Overview of PKI Trust Models", *IEEE Networks*, vol. 13, pp. 38 - 43, 1999.

[102] W. Tan, M. Yang, F. Ye, and W. Ren, "A Security Framework for Wireless Network Based on Public Key Infrastructure", *ISECS International Colloquium on Computing, Communication, Control, and Management,* vol. 2, pp. 567 - 570, 2009.

[103] D. Malan, M. Welsh, and M. Smith, "A Public-Key Infrastructure For Key Distribution in TinyOS Based on Elliptic Curve Cryptography", *in the Proceedings of the First Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks,* vol. 17, pp. 71 – 80, 2004 .

[104] W. Tan, W. Yang, M. Yang, F. Ye, and S. Zhang, "A Modification on Public Key Infrastructure Application", *International Conference on E-Business and Information System Security,* vol. 21, pp.1-4, Wuhan, 2009.

[105] D. Hu, D. Zhou, and P. Li, "PKI and Secret Key Based Mobile IP Security", *in the Proceedings of the International Conference on Communications, Circuits and Systems,* vol. 5, pp. 1605 – 1609, Guilin, 2006.

[106] N. Anuar, L. Kuen, O. Zakaria, and A. Gani, "Mobile Messaging Using Public Key Infrastructure: M-PKI", *in the Proceedings of the 12th WSEAS International Conference on Computers*, pp. 76-81, Greece, 2008.

[107] J. Buchmann, *Introduction to Cryptograph,* Second Ed.,Springer-Verlag, NY, LCC, USA, 2004.

[108] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, and A. Heckert, "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications", *NIST special publication 800-22*, 2001, [Online]. Available at: http://csrc.nist.gov/groups/ST/toolkit/rng/documents/SP800-22b.pdf.

[109] T. L. Win and N. C. Kyaw, "Speech Encryption and Decryption Using Linear Feedback Shift Register (LFSR)", *Journal World Academy Science, Engineering and Technology*, vol. 48, pp. 462-467, 2008.

[110] J. Shuman, "Multiple Packet-Streams in Encrypted Voice Over IP", Master of Science dissertation, Carleton University, Canada, 2003.

[111] R. Jain, *The Art of Computer Systems Performance Analysis: Techniques for Experimental Design, Measurement, Simulation, and Modeling*: John Wiley & Sons, Inc, 1991.

[112] S. Hassan and M. Kara, "Simulation-Based Performance Comparison of TCP-Friendly Congestion Control Protocols", *in the Proceedings of the 16th Annual UK Performance Engineering Workshop,* Durham, UK, 2000.

[113] A. Law and W. Kelto, *Simulation Modeling and Analysis*: McGraw-Hill, New York NY, USA, 1991.

[114] R.F. Sari, "Performance Evaluation of Active Network – Based Unicast and Multicast Congestion Control Protocols", PhD dissertation, Computer Science Department: University of Leeds, UK, 2004.

[115] W. Kehon, R. Sadowski, and D. Sturrock, "Simulation with Arena", McGraw-Hill Science/Engineering/Math, Mc-Graw-Hill, Inc, USA, 2004.

[116] K. Paw, H. Jeong, and J. Lee, "On Credibility of Simulation Studies of Telecommunication Networks", *IEEE Communications Magazine*, vol. 40, pp. 132-139, 2002.

[117] L. Bassham III, "Efficiency Testing of ANSI C Implementations of Round1 Candidate Algorithms for the Advanced Encryption Standard", *National Institute of Standards and Technology (NIST)*, 1999, [Online]. Available at: http:// csrc.nist.gov/archive/aes/round1/r1-ansic.pdf.

[118] G. Shepherd and D. Kruglinski, *Programming with Microsoft Visual C++. NET:* Sixth ed. Core Reference: Microsoft Pr, 2003.

[119] Z. Al-Sharif and C. Jeffery, "Adding High Level VoIP Facilities to the Unicon Language", *in the Proceedings of Third International Conference on Information Technology: New Generations*, vol. 4, pp. 524 - 529, Las Vegas, NV, 2006.

[120] J. Sifakis, S. Tripakis, and S. Yovine, "Building Models of Real-Time Systems From Application Software", *in the Proceedings of the IEEE*, vol. 91, pp. 100-111, 2003.

[121] G. Di Caro and M. Dorigo, "AntNet: Distributed Stigmergetic Control For Communications Networks", *Journal of Artificial Intelligence Research*, vol. 9, pp. 167, 1998.

[122] R. Fiach, *Network Programming in .NET With C# and Visual Basic .NET*, Elsevier Digital Press, 2004.

[123] X. Lai, J. Massey, and S. Murphy, "Markov Ciphers and Differential Cryptanalysis", *Advances in Cryptology-EUROCRYPT'91*, Springer-Verlag, vol. 547, pp. 17-38. 2000.

[124] C. Meyer, "Ciphertext/Plaintext and Ciphertext/Key Dependence vs. Number of Rounds for The Data Encryption Standard", *in the Proceedings of the National Computer Conference (afips)*, pp.11-19, 1978.

[125] M. El-Fotouh and K. Diepold, "Dynamic Substitution Model", *in the Proceedings of the Fourth International Conference on Information Assurance and Security (ISIAS'08)*, vol. 2, pp. 108-111, Naples, 2008.

[126] H. Phalgun, "The Effect of Voice Packet Size on End-To-End Delay in 802.11 b Networks", Master of Science dissertation, University of Pittsburgh, USA, 2003.

[127] T. Jamil, "The Rijndael Algorithm-A Brief Introduction to The New Encryption Standard", *IEEE Potentials*, vol. 23, pp. 36-38, 2004.

[128] R. Sever, A. Ismailglu, Y. Tekmen, M. Askar, and B. Okcan, "A High Speed FPGA Implementation of The Rijndael Algorithm", *in the Proceedings in the Euromicro Symposium on Digital System Design*, vol. 17, pp. 358 – 362, 2004.

[129] S. Tao, W. Ruli, and Y. Yixun, "Clock-Controlled Chaotic Key-Stream Generators", *Institution of Engineering and Technology Electronics Letters*, vol. 34, pp. 1932-1934, 1998.

[130] Ahmed, H. Kalash, and OSF, "Implementation of RC5 Block Cipher Algorithm for Image Cryptosystems", *International Journal of Information Technology*, vol. 3, pp. 245-250, 2008.

[131] W. Emm, "Impact of Multiencryption in Data Security", *International Journal of Computer Theory and Engineering*, vol. 1, pp. 571-567 , 2009.

[132] G. Marsaglia, "The Marsaglia Random Number CDROM Including The Diehard Battery of Tests of Randomness", 1995, [Online]. Available at: http://www.stat.fsu.edu/pub/diehard.

[133] J. Gleeson, "Truly Random Number Generator Based on Turbulent Electroconvection", *Journal of Applied Physics Letters*, vol. 81, pp. 1949-1952, 2002.

[134] E. John and J. Rubio, *Unique Chips and System*: Technology & Engineering, CRC Press, NY, USA 2007.

[135] S. Lee, H. Jeong, and Y. Lee, "Application-Adaptive Pseudo Random Number Generators and Binding Selector", *in the Proceedings of the 23rd International*

Technical Conferance on Circuits/Systems Computers and Communication (ITC-CSCC'08), vol. 27, pp. 1561-1564, 2008.

[136] M. Stipcevice, "The Diehard Battery of Stringent Statistical Randomness Tests", 2001, [Online]. Available at: http:// random.com.hr/products/random/manual/html/Diehard.htiml.

[137] R. Baldwin, "Preliminary Analysis of The BSAFE 3. x Pseudorandom Number Generators", *RSA Laboratories Bulletin* No. 8, 1998, [Online]. Available at: ftp://ftp.rsa.com/pub/pdfs/bulletn8.pdf.

[138] X. Zhang, K. Tang, and L. Shu, "A Chaotic Cipher Mmohocc and Its Randomness Evaluation", *in the Proceedings of the Sixth International Conference on Complex Systems: The New England Complex Systems Institute*, MA, Boston, 2006.

[139] B.-H. Kang, D.-H. Lee, and C.-P. Hong, "High-Performance Psedorandom Number Generator Using Two-Dimensional Cellular Automata," *in the Proceedings of the 4th IEEE International Symposium on Electronic Design, Test & Applications*, vol. 46, pp. 597-602, Hong Kong, 2008.

[140] A. Ephremides, "The Collected Papers of Claude E. Shannon", *Proceedings of IEEE*, vol. 84, pp. 1570-1571, 1996.

[141] C. Shannon, "Communication Theory of Secrecy Systems", *Bell Systems Technical Journal, MD Computing*, vol. 15, pp. 57-64, 1998.

[142] M. Alani, "Testing Randomness in Ciphertext of Block-Ciphers Using DieHard Tests", *International Journal of Computer Science and Network Security,* vol. 10, pp. 53-57, 2010.

[143] K. Tsoi, K. Leung, and P. Leong, "High Performance Physical Random Number Generator," *Computers & Digital Techniques IET*, vol. 1, pp. 349-352, 2007.

.[144] E. Lee, Y. They, S. Phang, H. Lim, and H. Lee, "Mutual Autonomy LFSR Output-Based Cellular Automata (MALO-CA)", *in the Proceedings of the IEEE International Conference on Convergence Information Technology*, pp. 1742-1745, Gyeongju, 2007.

[145] C. Sanchez-Avila and R. San, "The Rijndael Block Cipher (AES Proposal): A Comparison with DES", *in the Proceedings of the IEEE 35th Annual International Carnahan Conference on Security Technology*, pp. 229-234, London, 2001.

[146] L. Niansheng, G. Donghui, and H. Jiaxiang, "AES Algorithm Implemented for PDA Secure Communication with Java", *in the proceeding of the IEEE International Workshop on Anti-Counterfeiting, Security, Identification*, pp. 217 – 222, Xiamen, Fujian, 2007.

[147] K. Suwais, "Parallel Platform for New Secure Stream Cipher Based on NP-Hard Problems", PhD dissertation, Universiti Sains Malaysia (USM), Pineng, Malaysia, 2009.

[148] A. Masoun, "Cryptography Primitives Based on Piecewise Nonlinear Chaotic Maps", Master of Science dissertation, Universiti Sains Malaysia (USM), Pineng, Malaysia, 2008.

[149] A. Panato, M. Barcelos, and R. Reis, "A Low Device Occupation IP to Implement Rijndael Algorithm", *in the Proceedings of the Conference and Exhibition on Design, Automation and Test in Europe: Designers' Forum,* pp. 20 – 25, Brazil, 2003.

[150] A. Sterbenz and P. Lipp, "Performance of The AES Candidate Algorithms in Java", *in the Proceedings of the Third AES Candidate Conference, Printed by the National Institute of Standards and Technology (NIST)*, 2000.

[151] W. Wang, S. Liew, and V. Li, "Solutions To Performance Problems in VoIP Over a 802.11 Wireless LAN", *IEEE Transactions on Vehicular Technology*, vol. 54, pp. 366 – 384, 2005.

[152] C. Mucci, L. Vanzolini, F. Campi, and M. Toma, "Interactive Presentation: Implementation of AES/Rijndael on A Dynamically Reconfigurable Architecture", *in the Proceedings of the Conference and Exposition on Design, Automation and Test in Europe,* 2007.

[153] Kellerman Software, "What is The Strongest Encryption Algorithm?", July. 16, 2008, [Online]. Available at: http://www.kellermansoftware.com/tArticleStrongestAlgo.aspx [Accessed: June. 22, 2010].

[154] D. Elminaam, H. Kader, and M. Hadhoud, "Energy Efficiency of Encryption Schemes for Wireless Devices", *International Journal of Computer Theory and Engineering (IJCTE),* vol. 1, pp. 302-309, 2009.

[155] B. Carter, A. Kassin, and T. Magoc, "Symmetric Cryptosystems and Symmetric Key Management", 2007, [Online]. Available at: http://www.briancarter.info/pubs/symmetric_cryptosystems_and_symmetric_key_management.pdf.

[156] R. Rivest, M. Robshaw, R. Sidney, and Y. Yin, "The RC6 Block Cipher: AES Proposal", *National Institute of Standards and Technology (NIST),* 1998. [Online]. Available: http://csrc.nist.gov/archive/aes/round1/conf1/rc6.pdf.

[157] H. Ahmed, H. Kalash, and O. Allah, "Encryption Efficiency Analysis and Security Evaluation of RC6 Block Cipher for Digital Images", *in the Proceedings of the International Conference on Electrical Engineering*, vol. 3, pp. 33-39, Lahore, 2007.

[158] L. Elbaz and H. Bar-El, "Strength Assessment of Encryption Algorithms," *Advanced Security Solutions for Constrained Environments*, *Discretix Technologies*, Ltd., 2000.

[159] R. Rhouma, E. Solak, and S. Belghith, "Cryptanalysis of a New Substitution-Diffusion Based Image Cipher", *in the Proceedings of the Communications in Nonlinear Science and Numerical Simulation Conference*, vol. 15, pp. 1887-1892, 2010 .

[160] J. Beucha, "High Throughput Implementations of The RC6 Block Cipher Using Virtex-E and Virtex-II Block Cipher Using Virtex-E and Virtex-II", *Institut National De Recherche En informatique Et En Automatique,* 2002, [Online]. Available at: http://hal.archives-ouvertes.fr/docs/00/07/20/93/PDF/RR-4495.pdf.

[161] S. Contini, R. Yin, *The Security of the RC6 TM Block Cipher.* (MISC), 1998.

[162] H. Heys, "A Tutorial on Linear and Differential Cryptanalysis", *Electrical and Computer Engineering Cryptologia*, vol. 26, pp. 189-221, 2002.

[163] D. Lihua, Z. Yong, and H. Yupu, "F-GSS: A Novel FCSR-Based Keystream Generator", *in the Proceedings of the 1st International Conference on Information Science and Engineering (ICISE'09),* pp. 1737 – 1740, Nanjing, Jiangsu China, 2009.

[164] C. Lu, Y. Kan, H.Chiang, C. Yang, "Fast Implementation of AES Cryptographic Algorithms in Smart Cards", *in the Proceedings of the IEEE 37th Annual International Carnahan Conference on Security Technology,* pp. 573 – 579, 2003.

[165] D. McGrew and S. Fluhrer, "Attacks on Additive Encryption of Redundant Plaintext and Implications on Internet Security", *in Seventh Annual Workshop on Selected Areas in Cryptography*, pp. 14-28, 2000.

[166] A. Lashkari and M. Danesh, "A Survey on Wireless Security Protocols (WEP,WPA and WPA2/802.11i)", *in the Proceedings of the 2nd IEEE International Conference on Computer Science and Information Technology (ICCSIT'09),* pp. 48 – 52, Beijing, China, 2009.

[167] C. Li, S. Li, D. Zhang, G. Chen, "Cryptanalysis of A Data Security Protection Scheme for VoIP", *in the Proceedings of the IEE Vision, Image and Signal Processing*, vol. 153, pp. 1-10, 2006.

[168] C. Wang, M. Wen Li, W. Lian, "A Distributed Key-Changing Mechanism for Secure Voice Over IP (VoIP) Service", *in the Proceedings of the IEEE International Conference on Multimedia and Expo*, pp. 895-898, Beijing, 2007.

[169] H. Wang, "Skype VoIP Service- Architecture and Comparison", *INFOTECH Seminar Advanced Communication Services (ACS)*, 2005, [Online]. Available at: http://www.linecity.de/INFOTECH_ACS_SS05/acs5_top1_paper.pdf.

[170] G. Khaksari, A. Wijesinha, R. Karne, "Secure VoIP Using a Bare PC", *in the Proceedings of the 3rd International Conference on New Technologies, Mobility and Security (NTMS)*, pp. 1-5, Cairo, 2009.

[171] R. Rivest, M. Robshaw, R. Sidney, and Y. Yin, "The RC6™ Block Cipher", *RSA Laboratories*, No. 2955, 1998, [Online]. Available at: http://people.csail.mit.edu/rivest/Rc6.pdf

APPENDIX A

DIEHARD STATISTICAL TESTS SUITE

```
     NOTE: Most of the tests in DIEHARD return a p-value, which
     should be uniform on [0,1) if the input file contains truly
     independent random bits.  Those p-values are obtained by
     p=F(X), where F is the assumed distribution of the sample
     random variable X---often normal. But that assumed F is just
     an asymptotic approximation, for which the fit will be worst
     in the tails. Thus you should not be surprised with
     occasional p-values near 0 or 1, such as .0012 or .9983.
     When a bit stream really FAILS BIG, you will get p's of 0 or
     1 to six or more places.  By all means, do not, as a
     Statistician might, think that a p < .025 or p> .975 means
     that the RNG has "failed the test at the .05 level".  Such
     p's happen among the hundreds that DIEHARD produces, even
     with good RNG's.  So keep in mind that " p happens".
   ::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::
   ::            This is the BIRTHDAY SPACINGS TEST              ::
   :: Choose m birthdays in a year of n days.  List the spacings ::
   :: between the birthdays.  If j is the number of values that  ::
   :: occur more than once in that list, then j is asymptotically::
   :: Poisson distributed with mean m^3/(4n).  Experience shows n::
   :: must be quite large, say n>=2^18, for comparing the results::
   :: to the Poisson distribution with that mean.  This test uses::
   :: n=2^24 and m=2^9,  so that the underlying distribution for j::
   :: is taken to be Poisson with lambda=2^27/(2^26)=2.  A sample::
   :: of 500 j's is taken, and a chi-square goodness of fit test ::
   :: provides a p value.  The first test uses bits 1-24 (counting::
   :: from the left) from integers in the specified file.        ::
   ::   Then the file is closed and reopened. Next, bits 2-25 are::
   :: used to provide birthdays, then 3-26 and so on to bits 9-32.::
   :: Each set of bits provides a p-value, and the nine p-values ::
   :: provide a sample for a KSTEST.                             ::
   ::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::
BIRTHDAY SPACINGS TEST, M= 512 N=2**24 LAMBDA=  2.0000
         Results for ob.txt
                 For a sample of size 500:     mean
         ob.txt          using bits  1 to 24   2.076
 duplicate       number       number
 spacings       observed     expected
       0          56.       67.668
       1         142.      135.335
       2         136.      135.335
       3          85.       90.224
       4          50.       45.112
       5          21.       18.045
 6 to INF         10.        8.282
Chisquare with  6 d.o.f. =     4.02 p-value=  .325469
 ::::::::::::::::::::::::::::::::::::::::
                 For a sample of size 500:     mean
         ob.txt          using bits  2 to 25   2.030
 duplicate       number       number
 spacings       observed     expected
       0          58.       67.668
       1         142.      135.335
       2         128.      135.335
```

```
       3          103.        90.224
       4           44.        45.112
       5           18.        18.045
 6 to INF           7.         8.282
Chisquare with  6 d.o.f. =     4.14 p-value=  .342556
 ::::::::::::::::::::::::::::::::::::::::
                  For a sample of size 500:     mean
          ob.txt           using bits  3 to 26   1.880
 duplicate       number       number
 spacings       observed     expected
       0           69.        67.668
       1          150.       135.335
       2          145.       135.335
       3           75.        90.224
       4           37.        45.112
       5           18.        18.045
 6 to INF           6.         8.282
Chisquare with  6 d.o.f. =     6.96 p-value=  .675583
 ::::::::::::::::::::::::::::::::::::::::
                  For a sample of size 500:     mean
          ob.txt           using bits  4 to 27   1.928
 duplicate       number       number
 spacings       observed     expected
       0           63.        67.668
       1          138.       135.335
       2          163.       135.335
       3           74.        90.224
       4           43.        45.112
       5           11.        18.045
 6 to INF           8.         8.282
Chisquare with  6 d.o.f. =    11.81 p-value=  .933549
 ::::::::::::::::::::::::::::::::::::::::
                  For a sample of size 500:     mean
          ob.txt           using bits  5 to 28   2.040
 duplicate       number       number
 spacings       observed     expected
       0           68.        67.668
       1          138.       135.335
       2          129.       135.335
       3           90.        90.224
       4           42.        45.112
       5           19.        18.045
 6 to INF          14.         8.282
Chisquare with  6 d.o.f. =     4.56 p-value=  .399259
 ::::::::::::::::::::::::::::::::::::::::
                  For a sample of size 500:     mean
          ob.txt           using bits  6 to 29   1.948
 duplicate       number       number
 spacings       observed     expected
       0           73.        67.668
       1          148.       135.335
       2          118.       135.335
       3           89.        90.224
       4           48.        45.112
       5           15.        18.045
 6 to INF           9.         8.282
Chisquare with  6 d.o.f. =     4.60 p-value=  .404412
 ::::::::::::::::::::::::::::::::::::::::
```

```
                For a sample of size 500:      mean
          ob.txt          using bits  7 to 30   1.976
 duplicate        number        number
 spacings        observed     expected
       0           66.        67.668
       1          124.       135.335
       2          161.       135.335
       3           90.        90.224
       4           38.        45.112
       5           12.        18.045
 6 to INF           9.         8.282
Chisquare with  6 d.o.f. =     9.07 p-value=  .830121
 ::::::::::::::::::::::::::::::::::::::::
                For a sample of size 500:      mean
          ob.txt          using bits  8 to 31   1.968
 duplicate        number        number
 spacings        observed     expected
       0           60.        67.668
       1          153.       135.335
       2          131.       135.335
       3           85.        90.224
       4           48.        45.112
       5           17.        18.045
 6 to INF           6.         8.282
Chisquare with  6 d.o.f. =     4.49 p-value=  .389316
 ::::::::::::::::::::::::::::::::::::::::
                For a sample of size 500:      mean
          ob.txt          using bits  9 to 32   1.896
 duplicate        number        number
 spacings        observed     expected
       0           74.        67.668
       1          145.       135.335
       2          131.       135.335
       3           88.        90.224
       4           38.        45.112
       5           21.        18.045
 6 to INF           3.         8.282
Chisquare with  6 d.o.f. =     6.45 p-value=  .625303
 ::::::::::::::::::::::::::::::::::::::::
  The 9 p-values were
      .325469   .342556   .675583   .933549   .399259
      .404412   .830121   .389316   .625303
 A KSTEST for the 9 p-values yields  .506655

$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$

    ::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::
    ::            THE OVERLAPPING 5-PERMUTATION TEST                      ::
    :: This is the OPERM5 test.  It looks at a sequence of one mill-      ::
    :: ion 32-bit random integers.  Each set of five consecutive          ::
    :: integers can be in one of 120 states, for the 5! possible or-      ::
    :: derings of five numbers.  Thus the 5th, 6th, 7th,...numbers        ::
    :: each provide a state. As many thousands of state transitions       ::
    :: are observed,  cumulative counts are made of the number of         ::
    :: occurences of each state.  Then the quadratic form in the          ::
    :: weak inverse of the 120x120 covariance matrix yields a test        ::
    :: equivalent to the likelihood ratio test that the 120 cell          ::
    :: counts came from the specified (asymptotically) normal dis-        ::
```

```
     :: tribution with the specified 120x120 covariance matrix (with  ::
     :: rank 99).  This version uses 1,000,000 integers, twice.       ::
     ::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::
           OPERM5 test for file ob.txt
     For a sample of 1,000,000 consecutive 5-tuples,
 chisquare for 99 degrees of freedom= 82.858; p-value= .121306
           OPERM5 test for file ob.txt
     For a sample of 1,000,000 consecutive 5-tuples,
 chisquare for 99 degrees of freedom= 92.749; p-value= .342171
     ::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::
     :: This is the BINARY RANK TEST for 31x31 matrices. The leftmost ::
     :: 31 bits of 31 random integers from the test sequence are used ::
     :: to form a 31x31 binary matrix over the field {0,1}. The rank  ::
     :: is determined. That rank can be from 0 to 31, but ranks< 28   ::
     :: are rare, and their counts are pooled with those for rank 28. ::
     :: Ranks are found for 40,000 such random matrices and a chisqua-::
     :: re test is performed on counts for ranks 31,30,29 and <=28.   ::
     ::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::
    Binary rank test for ob.txt
         Rank test for 31x31 binary matrices:
        rows from leftmost 31 bits of each 32-bit integer
      rank   observed  expected (o-e)^2/e  sum
        28       238     211.4  3.342203    3.342
        29      5254    5134.0  2.804346    6.147
        30     22779   23103.0  4.545131   10.692
        31     11729   11551.5  2.726704   13.418
  chisquare=13.418 for 3 d. of f.; p-value= .996311
-------------------------------------------------------------
     ::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::
     :: This is the BINARY RANK TEST for 32x32 matrices. A random 32x ::
     :: 32 binary matrix is formed, each row a 32-bit random integer. ::
     :: The rank is determined. That rank can be from 0 to 32, ranks  ::
     :: less than 29 are rare, and their counts are pooled with those ::
     :: for rank 29.  Ranks are found for 40,000 such random matrices ::
     :: and a chisquare test is performed on counts for ranks  32,31, ::
     :: 30 and <=29.                                                  ::
     ::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::
    Binary rank test for ob.txt
         Rank test for 32x32 binary matrices:
        rows from leftmost 32 bits of each 32-bit integer
      rank   observed  expected (o-e)^2/e  sum
        29       206     211.4   .138848     .139
        30      5136    5134.0   .000771     .140
        31     23085   23103.0   .014097     .154
        32     11573   11551.5   .039926     .194
  chisquare=  .194 for 3 d. of f.; p-value= .351343
-------------------------------------------------------------

$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$

     ::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::
     :: This is the BINARY RANK TEST for 6x8 matrices.  From each of  ::
     :: six random 32-bit integers from the generator under test, a   ::
     :: specified byte is chosen, and the resulting six bytes form a  ::
     :: 6x8 binary matrix whose rank is determined.  That rank can be ::
     :: from 0 to 6, but ranks 0,1,2,3 are rare; their counts are     ::
     :: pooled with those for rank 4. Ranks are found for 100,000     ::
     :: random matrices, and a chi-square test is performed on        ::
```

```
:: counts for ranks 6,5 and <=4.                                        ::
::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::
    Binary Rank Test for ob.txt
   Rank of a 6x8 binary matrix,
rows formed from eight bits of the RNG ob.txt
b-rank test for bits  1 to  8
                OBSERVED   EXPECTED     (O-E)^2/E      SUM
     r<=4          930       944.3         .217        .217
     r =5        21658     21743.9         .339        .556
     r =6        77412     77311.8         .130        .686
                   p=1-exp(-SUM/2)= .29029
   Rank of a 6x8 binary matrix,
rows formed from eight bits of the RNG ob.txt
b-rank test for bits  2 to  9
                OBSERVED   EXPECTED     (O-E)^2/E      SUM
     r<=4          929       944.3         .248        .248
     r =5        21630     21743.9         .597        .845
     r =6        77441     77311.8         .216       1.060
                   p=1-exp(-SUM/2)= .41154
   Rank of a 6x8 binary matrix,
rows formed from eight bits of the RNG ob.txt
b-rank test for bits  3 to 10
                OBSERVED   EXPECTED     (O-E)^2/E      SUM
     r<=4          957       944.3         .171        .171
     r =5        21617     21743.9         .741        .911
     r =6        77426     77311.8         .169       1.080
                   p=1-exp(-SUM/2)= .41727
   Rank of a 6x8 binary matrix,
rows formed from eight bits of the RNG ob.txt
b-rank test for bits  4 to 11
                OBSERVED   EXPECTED     (O-E)^2/E      SUM
     r<=4          974       944.3         .934        .934
     r =5        21901     21743.9        1.135       2.069
     r =6        77125     77311.8         .451       2.520
                   p=1-exp(-SUM/2)= .71641
   Rank of a 6x8 binary matrix,
rows formed from eight bits of the RNG ob.txt
b-rank test for bits  5 to 12
                OBSERVED   EXPECTED     (O-E)^2/E      SUM
     r<=4          936       944.3         .073        .073
     r =5        21813     21743.9         .220        .293
     r =6        77251     77311.8         .048        .340
                   p=1-exp(-SUM/2)= .15650
   Rank of a 6x8 binary matrix,
rows formed from eight bits of the RNG ob.txt
b-rank test for bits  6 to 13
                OBSERVED   EXPECTED     (O-E)^2/E      SUM
     r<=4          891       944.3        3.009       3.009
     r =5        21774     21743.9         .042       3.050
     r =6        77335     77311.8         .007       3.057
                   p=1-exp(-SUM/2)= .78316
   Rank of a 6x8 binary matrix,
rows formed from eight bits of the RNG ob.txt
b-rank test for bits  7 to 14
                OBSERVED   EXPECTED     (O-E)^2/E      SUM
     r<=4          948       944.3         .014        .014
     r =5        21752     21743.9         .003        .018
     r =6        77300     77311.8         .002        .019
```

```
                  p=1-exp(-SUM/2)= .00961
   Rank of a 6x8 binary matrix,
rows formed from eight bits of the RNG ob.txt
b-rank test for bits  8 to 15
               OBSERVED   EXPECTED     (O-E)^2/E      SUM
     r<=4         989       944.3       2.116       2.116
     r =5       22040     21743.9       4.032       6.148
     r =6       76971     77311.8       1.502       7.650
                  p=1-exp(-SUM/2)= .97819
   Rank of a 6x8 binary matrix,
rows formed from eight bits of the RNG ob.txt
b-rank test for bits  9 to 16
               OBSERVED   EXPECTED     (O-E)^2/E      SUM
     r<=4         955       944.3         .121        .121
     r =5       22221     21743.9      10.468      10.590
     r =6       76824     77311.8       3.078      13.667
                  p=1-exp(-SUM/2)= .99892
   Rank of a 6x8 binary matrix,
rows formed from eight bits of the RNG ob.txt
b-rank test for bits 10 to 17
               OBSERVED   EXPECTED     (O-E)^2/E      SUM
     r<=4         913       944.3       1.038       1.038
     r =5       21894     21743.9       1.036       2.074
     r =6       77193     77311.8         .183       2.256
                  p=1-exp(-SUM/2)= .67636
   Rank of a 6x8 binary matrix,
rows formed from eight bits of the RNG ob.txt
b-rank test for bits 11 to 18
               OBSERVED   EXPECTED     (O-E)^2/E      SUM
     r<=4         895       944.3       2.574       2.574
     r =5       21630     21743.9         .597       3.171
     r =6       77475     77311.8         .344       3.515
                  p=1-exp(-SUM/2)= .82753
   Rank of a 6x8 binary matrix,
rows formed from eight bits of the RNG ob.txt
b-rank test for bits 12 to 19
               OBSERVED   EXPECTED     (O-E)^2/E      SUM
     r<=4         992       944.3       2.409       2.409
     r =5       21621     21743.9         .695       3.104
     r =6       77387     77311.8         .073       3.177
                  p=1-exp(-SUM/2)= .79578
   Rank of a 6x8 binary matrix,
rows formed from eight bits of the RNG ob.txt
b-rank test for bits 13 to 20
               OBSERVED   EXPECTED     (O-E)^2/E      SUM
     r<=4         929       944.3         .248        .248
     r =5       21705     21743.9         .070        .318
     r =6       77366     77311.8         .038        .356
                  p=1-exp(-SUM/2)= .16286
   Rank of a 6x8 binary matrix,
rows formed from eight bits of the RNG ob.txt
b-rank test for bits 14 to 21
               OBSERVED   EXPECTED     (O-E)^2/E      SUM
     r<=4         921       944.3         .575        .575
     r =5       21658     21743.9         .339        .914
     r =6       77421     77311.8         .154       1.069
                  p=1-exp(-SUM/2)= .41391
   Rank of a 6x8 binary matrix,
```

```
rows formed from eight bits of the RNG ob.txt
b-rank test for bits 15 to 22
                OBSERVED   EXPECTED     (O-E)^2/E      SUM
     r<=4          942       944.3         .006        .006
     r =5        21669     21743.9         .258        .264
     r =6        77389     77311.8         .077        .341
                   p=1-exp(-SUM/2)= .15663
   Rank of a 6x8 binary matrix,
rows formed from eight bits of the RNG ob.txt
b-rank test for bits 16 to 23
                OBSERVED   EXPECTED     (O-E)^2/E      SUM
     r<=4          987       944.3        1.931       1.931
     r =5        21632     21743.9         .576       2.507
     r =6        77381     77311.8         .062       2.569
                   p=1-exp(-SUM/2)= .72315
   Rank of a 6x8 binary matrix,
rows formed from eight bits of the RNG ob.txt
b-rank test for bits 17 to 24
                OBSERVED   EXPECTED     (O-E)^2/E      SUM
     r<=4          960       944.3         .261        .261
     r =5        21799     21743.9         .140        .401
     r =6        77241     77311.8         .065        .465
                   p=1-exp(-SUM/2)= .20763
   Rank of a 6x8 binary matrix,
rows formed from eight bits of the RNG ob.txt
b-rank test for bits 18 to 25
                OBSERVED   EXPECTED     (O-E)^2/E      SUM
     r<=4          962       944.3         .332        .332
     r =5        21691     21743.9         .129        .460
     r =6        77347     77311.8         .016        .476
                   p=1-exp(-SUM/2)= .21197
   Rank of a 6x8 binary matrix,
rows formed from eight bits of the RNG ob.txt
b-rank test for bits 19 to 26
                OBSERVED   EXPECTED     (O-E)^2/E      SUM
     r<=4          990       944.3        2.212       2.212
     r =5        21716     21743.9         .036       2.247
     r =6        77294     77311.8         .004       2.251
                   p=1-exp(-SUM/2)= .67558
   Rank of a 6x8 binary matrix,
rows formed from eight bits of the RNG ob.txt
b-rank test for bits 20 to 27
                OBSERVED   EXPECTED     (O-E)^2/E      SUM
     r<=4          919       944.3         .678        .678
     r =5        21736     21743.9         .003        .681
     r =6        77345     77311.8         .014        .695
                   p=1-exp(-SUM/2)= .29356
   Rank of a 6x8 binary matrix,
rows formed from eight bits of the RNG ob.txt
b-rank test for bits 21 to 28
                OBSERVED   EXPECTED     (O-E)^2/E      SUM
     r<=4          897       944.3        2.369       2.369
     r =5        21828     21743.9         .325       2.695
     r =6        77275     77311.8         .018       2.712
                   p=1-exp(-SUM/2)= .74233
   Rank of a 6x8 binary matrix,
rows formed from eight bits of the RNG ob.txt
b-rank test for bits 22 to 29
```

```
                  OBSERVED   EXPECTED     (O-E)^2/E      SUM
      r<=4           968       944.3         .595         .595
      r =5         21554     21743.9        1.658        2.253
      r =6         77478     77311.8         .357        2.611
                     p=1-exp(-SUM/2)= .72890
    Rank of a 6x8 binary matrix,
  rows formed from eight bits of the RNG ob.txt
  b-rank test for bits 23 to 30
                  OBSERVED   EXPECTED     (O-E)^2/E      SUM
      r<=4           956       944.3         .145         .145
      r =5         21922     21743.9        1.459        1.604
      r =6         77122     77311.8         .466        2.070
                     p=1-exp(-SUM/2)= .64472
    Rank of a 6x8 binary matrix,
  rows formed from eight bits of the RNG ob.txt
  b-rank test for bits 24 to 31
                  OBSERVED   EXPECTED     (O-E)^2/E      SUM
      r<=4           983       944.3        1.586        1.586
      r =5         22005     21743.9        3.135        4.721
      r =6         77012     77311.8        1.163        5.884
                     p=1-exp(-SUM/2)= .94723
    Rank of a 6x8 binary matrix,
  rows formed from eight bits of the RNG ob.txt
  b-rank test for bits 25 to 32
                  OBSERVED   EXPECTED     (O-E)^2/E      SUM
      r<=4           978       944.3        1.203        1.203
      r =5         21926     21743.9        1.525        2.728
      r =6         77096     77311.8         .602        3.330
                     p=1-exp(-SUM/2)= .81081
  TEST SUMMARY, 25 tests on 100,000 random 6x8 matrices
 These should be 25 uniform [0,1] random variables:
    .290289     .411535     .417267     .716410     .156499
    .783164     .009607     .978185     .998923     .676364
    .827534     .795785     .162858     .413908     .156628
    .723145     .207631     .211972     .675584     .293561
    .742333     .728898     .644718     .947235     .810811
  brank test summary for ob.txt
      The KS test for those 25 supposed UNI's yields
                 KS p-value= .588188

$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$

    ::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::
    ::                     THE BITSTREAM TEST                               ::
    :: The file under test is viewed as a stream of bits. Call them  ::
    :: b1,b2,... .  Consider an alphabet with two "letters", 0 and 1 ::
    :: and think of the stream of bits as a succession of 20-letter  ::
    :: "words", overlapping.  Thus the first word is b1b2...b20, the ::
    :: second is b2b3...b21, and so on.  The bitstream test counts   ::
    :: the number of missing 20-letter (20-bit) words in a string of ::
    :: 2^21 overlapping 20-letter words.  There are 2^20 possible 20 ::
    :: letter words.  For a truly random string of 2^21+19 bits, the ::
    :: number of missing words j should be (very close to) normally  ::
    :: distributed with mean 141,909 and sigma 428.  Thus            ::
    ::  (j-141909)/428 should be a standard normal variate (z score) ::
    :: that leads to a uniform [0,1) p value.  The test is repeated  ::
    :: twenty times.                                                 ::
    ::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::
```

```
 THE OVERLAPPING 20-tuples BITSTREAM  TEST, 20 BITS PER WORD, N words
   This test uses N=2^21 and samples the bitstream 20 times.
  No. missing words should average  141909. with sigma=428.
---------------------------------------------------------
 tst no  1:  142952 missing words,    2.44 sigmas from mean, p-value=
.99258
 tst no  2:  141406 missing words,   -1.18 sigmas from mean, p-value=
.11980
 tst no  3:  142597 missing words,    1.61 sigmas from mean, p-value=
.94594
 tst no  4:  141682 missing words,    -.53 sigmas from mean, p-value=
.29766
 tst no  5:  141581 missing words,    -.77 sigmas from mean, p-value=
.22150
 tst no  6:  142439 missing words,    1.24 sigmas from mean, p-value=
.89206
 tst no  7:  142887 missing words,    2.28 sigmas from mean, p-value=
.98882
 tst no  8:  142260 missing words,     .82 sigmas from mean, p-value=
.79370
 tst no  9:  142120 missing words,     .49 sigmas from mean, p-value=
.68872
 tst no 10:  141938 missing words,     .07 sigmas from mean, p-value=
.52671
 tst no 11:  141982 missing words,     .17 sigmas from mean, p-value=
.56741
 tst no 12:  141519 missing words,    -.91 sigmas from mean, p-value=
.18089
 tst no 13:  141523 missing words,    -.90 sigmas from mean, p-value=
.18336
 tst no 14:  141007 missing words,   -2.11 sigmas from mean, p-value=
.01750
 tst no 15:  142010 missing words,     .24 sigmas from mean, p-value=
.59298
 tst no 16:  141524 missing words,    -.90 sigmas from mean, p-value=
.18398
 tst no 17:  142232 missing words,     .75 sigmas from mean, p-value=
.77455
 tst no 18:  141859 missing words,    -.12 sigmas from mean, p-value=
.45320
 tst no 19:  142296 missing words,     .90 sigmas from mean, p-value=
.81685
 tst no 20:  141548 missing words,    -.84 sigmas from mean, p-value=
.19927

$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$

     :::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::
     ::             The tests OPSO, OQSO and DNA                        ::
     ::         OPSO means Overlapping-Pairs-Sparse-Occupancy           ::
     :: The OPSO test considers 2-letter words from an alphabet of      ::
     :: 1024 letters.  Each letter is determined by a specified ten     ::
     :: bits from a 32-bit integer in the sequence to be tested. OPSO   ::
     :: generates  2^21 (overlapping) 2-letter words  (from 2^21+1      ::
     :: "keystrokes")  and counts the number of missing words---that    ::
     :: is 2-letter words which do not appear in the entire sequence.   ::
     :: That count should be very close to normally distributed with    ::
     :: mean 141,909, sigma 290. Thus (missingwrds-141909)/290 should   ::
```

```
    :: be a standard normal variable. The OPSO test takes 32 bits at ::
    :: a time from the test file and uses a designated set of ten    ::
    :: consecutive bits. It then restarts the file for the next de-  ::
    :: signated 10 bits, and so on.                                  ::
    ::                                                               ::
    ::     OQSO means Overlapping-Quadruples-Sparse-Occupancy         ::
    ::   The test OQSO is similar, except that it considers 4-letter ::
    :: words from an alphabet of 32 letters, each letter determined  ::
    :: by a designated string of 5 consecutive bits from the test    ::
    :: file, elements of which are assumed 32-bit random integers.   ::
    :: The mean number of missing words in a sequence of 2^21 four-  ::
    :: letter words,  (2^21+3 "keystrokes"), is again 141909, with   ::
    :: sigma = 295.  The mean is based on theory; sigma comes from   ::
    :: extensive simulation.                                         ::
    ::                                                               ::
    ::    The DNA test considers an alphabet of 4 letters:: C,G,A,T,::
    :: determined by two designated bits in the sequence of random   ::
    :: integers being tested.  It considers 10-letter words, so that ::
    :: as in OPSO and OQSO, there are 2^20 possible words, and the   ::
    :: mean number of missing words from a string of 2^21  (over-    ::
    :: lapping)  10-letter  words (2^21+9 "keystrokes") is 141909.   ::
    :: The standard deviation sigma=339 was determined as for OQSO   ::
    :: by simulation.  (Sigma for OPSO, 290, is the true value (to   ::
    :: three places), not determined by simulation.                  ::
    ::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::
OPSO test for generator ob.txt
 Output: No. missing words (mw), equiv normal variate (z), p-value (p)
                                                          mw      z      p
   OPSO for ob.txt          using bits 23 to 32        142138   .789
.7848
   OPSO for ob.txt          using bits 22 to 31        142013   .357
.6396
   OPSO for ob.txt          using bits 21 to 30        142314  1.395
.9186
   OPSO for ob.txt          using bits 20 to 29        141651  -.891
.1865
   OPSO for ob.txt          using bits 19 to 28        141833  -.263
.3962
   OPSO for ob.txt          using bits 18 to 27        141856  -.184
.4270
   OPSO for ob.txt          using bits 17 to 26        141711  -.684
.2470
   OPSO for ob.txt          using bits 16 to 25        141632  -.956
.1695
   OPSO for ob.txt          using bits 15 to 24        140958 -3.280
.0005
   OPSO for ob.txt          using bits 14 to 23        141815  -.325
.3725
   OPSO for ob.txt          using bits 13 to 22        141878  -.108
.4570
   OPSO for ob.txt          using bits 12 to 21        141205 -2.429
.0076
   OPSO for ob.txt          using bits 11 to 20        141947   .130
.5517
   OPSO for ob.txt          using bits 10 to 19        141618 -1.005
.1575
   OPSO for ob.txt          using bits  9 to 18        141610 -1.032
.1510
```