Smile Mask
Development of Cryptography Performance of MOLAZ Method (MOLAZ-SM)

A project submitted to the School of computing in partial fulfillment of the requirements for the degree of Master of Science (Information Technology)
Universiti Utara Malaysia

By

Moceheb Lazam Shuwandy (802860)

Copyright © Moceheb Lazam, 2012. All rights reserved.

KOLEJ SASTERA DAN SAINS
(College of Arts and Sciences)
Universiti Utara Malaysia

PERAKUAN KERJA KERTAS PROJEK
(Certificate of Project Paper)

Saya, yang bertandatangan, memperakukan bahawa
(I, the undersigned, certifies that)

MOCEHEB LAZAM SHUWANDY
(802860)

calon untuk Ijazah
(candidate for the degree of) **MSc. (Information Technology)**

telah mengemukakan kertas projek yang bertajuk
(has presented his/her project of the following title)

SMILE MASK DEVELOPMENT OF CRYPTOGRAPHY PERFORMANCE OF MOLAZ METHOD (MOLAZ-SM)

seperti yang tercatat di muka surat tajuk dan kulit kertas projek
(as it appears on the title page and front cover of project)

bahawa kertas projek tersebut boleh diterima dari segi bentuk serta kandungan dan meliputi bidang ilmu dengan memuaskan.
(that this project is in acceptable form and content, and that a satisfactory knowledge of the field is covered by the project).

Nama Penyelia
(Name of Supervisor) : **ASSOC. PROF. DR. WAN ROZAINI SHEIK OSMAN**

Tandatangan
(Signature) : Rozaini Tarikh (Date) : 31/1/2012

ASSOC. PROF. DR. WAN ROZAINI SHEIK OSMAN
DIRECTOR
ITU-UUM ASP CoE For Rural ICT Development
CONVENTION COMPLEX
UNIVERSITI UTARA MALAYSIA
06010 UUM SINTOK
KEDAH DARUL AMAN, MALAYSIA

Nama Penilai
(Name of Evaluator) : **DR. KANG ENG THYE**

Tandatangan
(Signature) : _____ Tarikh (Date) : 29/1/2012

DR. KANG ENG THYE
Senior Lecturer
School of Computing
UUM College of Arts and Sciences
Universiti Utara Malaysia

PERMISSION TO USE

In presenting this project in partial fulfillment 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 copying of this project in any manner, in whole or in part, for scholarly purposes may be granted by my supervisor in her absence, by the Dean of the School of Computing. It is understood that any copying or publication or use of this project or parts thereof for financial gain should 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 project.

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

Dean of School of Computing
Universiti Utara Malaysia
06010 UUM Sintok
Kedah Darul Aman

ABSTRACT

Concealment of information is the most important things of interest to scientists and users alike. The work of many researchers to find new ways and methods for building specialized systems to protect the information from hackers. The method of those techniques AES and an adopted by the U.S. Department of Defense and launched in the eighties to the world. Even so, it parallels the evolution of these methods to penetrate systems. Researchers were developed this method for the protection of this algorithm. In the end of 2010 the researcher Engineer Moceheb Lazam during his studies at the Masters in the Universiti Utara Malaysia, develop this algorithm in order to keep the encryption and decoding. It was called MOLAZ. It used two algorithms AES 128 and AES 256 bits, and switching between them using special key (K_s). In addition, it uses two keys to encryption and decryption. However, this method needs to be develops and supports the protection of information. Therefore, in 2011 appeared MOLAZ-SM. It presents a study is the development of this system by adding the mask technique to prevent the use of the style of repeated attempts to enter the key. The system depends on the base "If you enter a true key, you obtain to the truth information, but if you enter the false key; you obtains to the false information."

ACKNOWLEDGEMENTS

I would like to offer my sincere thanks to my supervisor Assoc. Prof. Dr. Wan Rozaini Bt Sheik Osman for her excellent guidance and moral support, her time and her patience and commitment in helping me complete this research. I don't forget my brother and my co-supervisor Dr. Massudi Mahmuddin for his perfect guidance and support.

I would like hardly to say thanks to my brother Dr. Adib M. Monzer Habbal to his great guidance. I don't forget the hero who helps me and gives his hand to make this research in perfect case, Dr. Fadi Maher Saleh Alkhasawneh.

I would also like to offer my deepest gratitude to my family for helping me, and for encouraging me to do my master 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 of 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 completing this research.

Table of Contents

List of tables

List of Figures

List of Abbreviations

AES	**A**dvanced **E**ncryption **S**tandard
AES-128	128 bits is the size of key
AES-256	256 bits is the size of key
CAST	**C**arlisle **A**dams, **S**tafford **T**avares
DES	**D**ata **E**ncryption **S**tandard
GC	**G**arbage **C**ollection
JVM	**J**ava **V**irtual **M**achine
K_s	**S**ecret **K**ey generates randomly
LS	**L**uck **S**ystem
MLZ	**MOLAZ** extension of encrypted file
MOLAZ	**M**oceheb **L**azam
MOLAZ-SM	**MOLAZ-S**mile **M**ask system
SDA	**S**equence **D**etermine **A**lgorithm
SMS	**S**mile **M**ask **S**ystem
VM	**V**irtual **M**achine
BFA	**B**rute **F**orce **A**ttack

CHAPTER ONE
INTRODUCTION

1.1 Background

Cryptosystems are classified into two types symmetric (secret-key) and asymmetric (public-key). Improved security is the main objective of encryption. At any time, private keys do not need to be sent or shown to anyone. In a secret-key system, by disparity the secret keys' necessity be transmitted (either by hand or through a transmission channel) since the duplicate key is used for encryption and decryption. The possibility of detecting the secret key during transference is very high by enemies. Another foremost advantage of public-key systems is that they can give digital signatures that cannot be denied. Authentication through secret-key systems needs sharing of some secret and from time to time requires trust of a third party as well.

As a result, a transmitter can repudiate previous authenticated message by claiming the shared secret was somehow compromised by one of the parties sharing the secret (Simmons, 1992). For example, authentication system of the Kerberos secret-key involves a central database that keeps copies of the secret keys of all users; an attack on the database would allow widespread forgery. Authentication of public-key, prevents this type of repudiation; each user has sole responsibility for protecting his or her private key (EMC, 2011). For examples of asymmetric key algorithms include NTRUEncrypt cryptosystem and McEliece cryptosystem, and for symmetric key algorithms include Twofish, Serpent and AES (Rijndael).

The contents of the thesis is for internal user only

REFERENCES

Adams, C., Heys, H., Tavares, S. & Wiener M. (1999). An analysis of the CAST-256 cipher. IEEE .22(1)

Ali, N. B. Z., and Noras, J. M. (2001). Optimal Data Path Design for a Cryptographic Processor. The Blowfish Algorithm. *Malaysian Journal of Computer Science*, 14(1), 6853-6862.

Anderson R., Biham E. & Knudsen L. (1998). *Serpent: A proposal for the advanced encryption standard.* NIST AES Proposal .

Beaver, K. (2006). *Hacking For Dummies.* Indianapolis, Indiana: Wiley.

Biryukov A., & Khovratovich D. (2009). Related-key Cryptanalysis of the Full AES-192 and AES-256. *Advances in Cryptology–ASIACRYPT* , 1-18.

Bruce S., John K., Doug W., David W., Chris H., Niels F., Tadayoshi K.& Mike S., (2000). "*The Twofish Team's Final Comments on AES Selection*". Retrieved (12/10/2011) from (http://www.schneier.com/paper-twofish-final.pdf) . http://www.schneier.com/paper-twofishfinal.pdf .

Carter B., Kassin A., & Magoc T. (2007). Advanced Encryption Standard. *CiteSeerX.* 10.1.1.135.1231

Chih-Chung L. & Shau-Yin T.. (2010). Integrated Design of AES (Advanced Encryption Standard) Encrypter and Decrypter. Hsinchu, Taiwan: *Industrial Technology Research Institute.*

Coppersmith, D. (1994). The Data Encryption Standard (DES) and its strength against attacks. *IBM Journal of Research and Development* 38 (3), 243.

Daemen J.& RijnMen V., (1998). The Rijndael Block Cipher. *First AES Candidate Conference (AES1)* (pp. 20-22). AES proposal.

Daemen J., & Rijmen V. (1999). AES Proposal: Rijndael. AES Algorithm Submission, *First AES Candidate Conference (AES1)* (pp. 20-22). AES proposal..

Danny C. (2010). *DES Encryption*, Retrieved (20/10/2011) from http://www.dannycrichton.com/wp-content/uploads/2010/07/ Crichton-DES-Essay.pdf .

David H. (2005). Beginning Cryptography with Java. *Wrox* .

Davidson B., Luiz C. and Raphael M. (2011). Brute force attacks against reflection-based software integrity verification methods. *Universidade Federal do Rio de Janeiro (UFRJ)*, 1-8, Brazil.

Diaa S., Hatem M., & Mohiy M. (2010). Evaluating The Performance of Symmetric Encryption Algorithms. *IJCSNS International Journal of Computer Science and Network Security* , 10(3), 216–222. APA 6th edition.

EMC (2011), New Attack on AES. RSA Share Project, *EMC Corporation* , Retrieved(15/9/2011) from https://community.emc.com/community/edn/rsashare/blog/2011/08/31/new-attack-on-aes.

Federal Information Processing Standards Publication 197. (2001). *Advanced Encryption Standard (AES)*. Nov. 26.

Gladman, B. (2002). A Specification for the AES Algorithm. Berkeley.

Ichikawa T., Kasuya T., Matsui M. (2000). Hardware Evaluation of the AES finalists. The Third Advanced EncryptionStandard (AES3*) Candidata Conference.*

James N., Elaine B., Lawrence B., William B., Morris D., James F.,& Edward R. (2000). Report on the development of the Advanced Encryption Standard (AES). *Journal of Research-National Institute of Standards and Technology* , 3(106),511-576.

Jason W. (2004). *Java Cryptography Extensions: Practical Guide for Programmers (The Practical Guides)*. Morgan Kaufmann .

Jim H., (2011). Explanation of AES, Retrieved (5/11/2011) from http://www.giac.org/cissp-papers/67.pdf .

Jonathan B.,& Knud S. (1998). *Java Cryptography*. Oreilly,First Edition.

Joost, K. (2011). Practical hacking AES using the S-box weakness. *IN DEI NOMINE FELICITER*. Russia. Retrieved (6/10/2011) from http://www.cs.ru.nl/bachelorscripties/2011/Joost_Kremers___0714402___Practical_hacking_AES_using_the_S-box_weakness.pdf

Khadivi, P. ,& Momtazpour, M. (2009). Application of data mining in cryptanalysis. Communications and Information Technology, *9th International Symposium on* , 28-30.

Kuechler, B., & Vaishnavi, V. (2008). On theory development in design science research: anatomy of a research project. *European Journal of Information Systems,* 17(5), 489-504.

L-3 Communications Cincinnati Electronics (2006). "AES-256 Encryption Core Security Policy", Information Technology Laboratory, *National Institute of Standards and Technology.*

Lee. A. (2007). *Guideline for Implementing Cryptography in the Federal Government.* Retrieved (12/10/2011) from National Institute of Standards and Technology: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

Liberatori, M. , Otero, F. , Bonadero, J.C. , Castineira, J. (2007). AES-128 Cipher. High Speed, Low Cost FPGA Implementation. Programmable Logic, SPL '07. *3rd Southern Conference.*

Luis M. ,& Cortés P. (2005). SeChat: An AES Encrypted Chat. Retrieved (5/10/2010) from http://users.ece.gatech.edu/~cortes/SeChat/SeChat.pdf

Moceheb L., Ali K., Firas L., & Adib M. (2010). Switching between the AES-128 and AES-256 Using Ks * & Two Keys (MOLAZ Method*). IJCSNS International Journal of Computer Science and Network Security*, 8(11).

Naziri, S. & Idris, N. (2008). The memory-less method of generating multiplicative inverse values for S-box in AES algorithm. *IEEE* .

NIST, (2000). AES page available via. Retrieved (8/9/2011) from http://www.nist.gov/CryptoToolkit

Oracle Sun Developer Network, Lesson 3: Cryptography. (2010). Cryptography. Retrieved (6/11/2011) from Oracle Sun Developer: http://java.sun.com/developer/onlineTraining/Programming/BasicJava2/crypto.html

Ors, S., Gurkaynak, F., Oswald, E. & Preneel, B. (2001). Power-Analysis Attack on an ASIC AES implementation. IEEE, City .

Rudra, A., Dubey, P. K., Jutla, C. S., Kumar, V., Rao, J. R. & Rohatgi, P. (2001). *Efficient Rijndael Encryption Implementation with Composite Field Arithmetic.* Berlin Heidelberg: Springer-Verlag.

Sanchez, C., Avila, K., & Reillo, S. (2001). The Rijndael Block Chiper (AES Proposal): A Comparison with DES. IEEE.

Satoh, A. & Morioka, S.(2003). *Unified Hardware Architecture for 128-Bit Block Ciphers AES and Camellia.* Berlin Heidelberg: Springer-Verlag.

Seagate Technology LLC. (2010). 128-Bit Versus 256-Bit AES Encryption. Retrieved (10/10/2011) from *Seagate*: www.seagate.com/staticfiles/.../tp596_128-bit_versus_256_bit.pdf

Selent D. (2010). Advanced Encryption Standard. *Rivier Academic Journal*, 6(2).

Shu J., Wang Y., Wenchang Li W. & Zhiyong Z. (2010). Realization Of A Resouce Sharing Fast Encryption and Decryption AES Algorithm. *Journal of International Symposium on Intelligent Signal Processing and Communication Systems* (ISPACS 2010) .

Simmons G.J. (1992). *Contemporary Cryptology, The Science of Information Integrity.* IEEE, New York.

Srinivasan, S. (2006). Security and Privacy in the Computer Forensics Context. Communication Technology, 2006. ICCT '06. *International Conference* , 1 - 3 .

Steve A., & Robbert F. (2009). How to hide information for later use on networks. *IEEE* , 653 - 657.

Wang C. & Heys H. (2009). Using a pipelined S-box in compact AES hardware implementations. 101-104.

Westlund L., Harold B. (2002). "NIST reports measurable success of Advanced Encryption Standard". *Journal of Research of the National Institute of Standards and Technology.*

William S. (2010). *Cryptography and network security-principles and Practices*, Prentice Hall of India, 3 rd Edition.

Zimmermann, P. (1995). *PGP Source Code and Internals. MIT Press.*