ANALYSIS AND MODIFICATION OF GRAIN - 128 STREAM CIPHER ALGORITHM

Norul Hidayah Binti Lot @ Ahmad Zawawi
(Matric No. 3110120)

Thesis submitted in fulfilment for the degree of
MASTER OF SCIENCE
INFORMATION SECURITY AND ASSURANCE

Faculty of Science and Technology
UNIVERSITI SAINS ISLAM MALAYSIA
Nilai

July 2015

AUTHOR DECLARATION

I hereby declare that the work in this thesis is my own except for quotations and summaries which have been duly acknowledged

Date :

Signature :
Name : Norul Hidayah Bt. Lot @ Ahmad Zawawi
Matric No : 3110120
Address : No 3 Jalan Polo Air, 13/57 Seksyen 13
40100 Shah Alam Selangor

BIODATA OF AUTHOR

Norul Hidayah Binti Lot @ Ahmad Zawawi (3110120) was born on the 18th December 1983. She is currently working at CyberSecurity Malaysia, who involved in research and development in cyber technologies related field (specialized in cryptography). She previously was a student of UiTM and obtained Bachelor of Science (Hons) Management Mathematics from Faculty of Information Technology & Quantitative Sciences (currently known as Computer & Mathematical Sciences). She is at present a part-time Master student of USIM majoring in Cryptography.

ACKNOWLEDGEMENTS

In the name of Allah, the Beneficent, the Merciful. Praise be to Allah, Lord of the Worlds. I want to take this chance to acknowledge the contribution, assistance and support of several people who help to complete my research project.

I would like to express my appreciation to my supervisor, Prof. Dr. Kamaruzzaman bin Seman and my co - supervisor Dr Nurzi Juana binti Mohd Azizi for the continued support and guidance during the research.

I would like to extend my appreciation to my lecturers, Prof Madya Dr Zaiton binti Hassan and Dr Mohd Kidin bin Shahran for their invaluable sources of knowledge and advices.

I also would like to extend my gratitude to Universiti Sains Islam Malaysia (USIM) for giving me chances to further study in my Master program to gain knowledge and experience.

Special thanks to my husband, parents and also family members for their prayers, patience, understanding and support during the entire of my study.

Finally, thanks also to my colleague in CTR Department of CyberSecurity Malaysia and all my friends in USIM for their assisting and guidance for this research project becomes successful.

ABSTRAK

Tesis ini membentangkan tentang algoritma stream cipher yang baru. Algoritma stream cipher yang baru ini merupakan satu usul yang berdasarkan kepada algoritma yang sedia ada iaitu algoritma Grain-128 stream cipher. Dalam mencapai tujuan pembentangan ini, terdapat tiga objektif utama yang dibentangkan. Objektif yang pertama bagi kajian ini ialah untuk mengenalpasti kerawakan algoritma Grain-128 stream cipher. Seterusnya, pengubahsuaian terhadap algoritma Grain-128 stream cipher akan dilaksanakan untuk menghasilkan algoritma stream cipher yang baru. Dan yang terakhir, ujian kerawakan terhadap algoritma Modified Grain-128 stream cipher dilaksanakan untuk menentukan samada algoritma yang baru ini adalah rawak atau tidak. Perbandingan antara algoritma Grain-128 dan Modified Grain-128 akan dinilai dengan menggunakan NIST Statistical Test Suite. NIST Statistical Test Suite ini telah dibangunkan hasil kerjasama diantara Bahagian Keselamatan Komputer (Computer Security Division) dan Bahagian Kejuruteraan Statistik (Statistical Engineering Division) di Institut Piawaian dan Teknologi Kebangsaan (Nasional Institute of Standard and Technology, NIST). NIST Statistical Test Suite ini dilaksanakan bagi menentukan kerawakan terhadap kedua-dua algoritma tersebut. Kesimpulannya, algoritma Modified Grain-128 stream cipher adalah lebih rawak berbanding algoritma Grain-128 stream cipher berdasarkan tahap signifikan 1%-5%.

ABSTRACT

This thesis presents a new stream cipher algorithm. The new stream cipher algorithm have been proposed based on the existing Grain - 128 stream cipher algorithm. There are three main objectives in order to achieve this purpose. The first objective of this research is to identify the randomness of Grain – 128 stream cipher algorithm. Next, the modification of the algorithm will be conducted against Grain - 128 stream cipher algorithm. Finally, the randomness testing of Modified Grain – 128 of stream cipher algorithm is conducted to determine whether this algorithm is random or not random. The comparison of Grain - 128 and Modified Grain - 128 will be evaluated by using NIST Statistical Test Suite. The NIST Statistical Test Suite was developed by collaboration between the Computer Security Division and the Statistical Engineering Division at National Institute of Standard and Technology (NIST). The NIST Statistical Test Suite is conducted to determine the randomness of both algorithms. Conclusively, the Modified Grain - 128 is random based on 1% - 5% of significance level compared to the Grain - 128 which is not random at the same significance level.

ملخص

تقدم هذه الرسالة الخوارزمية تيار الشفرات الجديدة .لقد تم اقتراح خوارزمية تيار الشفرات جديدة تقوم على الحبوب الموجودة - خوارزمية التشفير 128تيار .هناك ثلاثة أهداف رئيسية لتحقيق هذا الغرض .الهدف الأول من هذا البحث هو التعرف على العشوائية من الحبوب 128 -تيار خوارزمية تشفير .وبعد ذلك، سيتم إجراء تعديل خوارزمية ضد الحبوب 128 -تيار خوارزمية تشفير .وأخيرا، فإن الاختبارات العشوائية من الحبوب المعدلة -وأجرى 128من خوارزمية تيار والشفرات لتحديد ما إذا كان هذا الخوارزمية عشوائية أو غير عشوائي .وسيتم تقييم 128باستخدام NISTالإحصائية اختبار جناح -المقارنة من الحبوب 128 - والتعديل الحبوب .وقد تم تطوير NISTالإحصائية اختبار جناح من التعاون بين شعبة الهندسة الإحصائية في المعهد الوطني للستاندرد والتكنولوجيا (NIST) شعبة أمن الحاسوب و .وأجرى NISTالإحصائية اختبار جناح لتحديد العشوائية في كل من الخوارزميات .قاطع، والحبوب المعدلة 128 -هو عشوائي على أساس ٪5 - ٪1من مستوى الأهمية بالمقارنة مع الحبوب 128 - وهي ليست عشوائية عند مستوى الدلالة نفسه.

CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

NIST	-	National Institute of Standards and Technology
IV	-	Initial Value
LFSR	-	Linear Feedback Shift Register
NLFSR	-	Non-Linear Feedback Shift Register
MG-128	-	Modified Grain-128
DSA	-	Digital Signature Algorithm
AES	-	Advanced Encryption Standard
DES	-	Data Encryption Standard
IDEA	-	International Data Encryption Algorithm
RC4	-	Rivest Cipher 4
FISH	-	FIbonacci SHrinking
XOR	-	Exclusive-or
SPRNG	-	Scalable Parallel Pseudorandom Number Generator
GUI	-	Graphical User Interface
DFT	-	Discrete Fourier Transform