IMPLEMENTATION AND INTEGRATION OF HF MESSAGING SYSTEM WITH CRYPTOGRAPHIC FEATURES

ABD RAHIM B MAT SIDEK

A thesis submitted in fulfilment of the
requirements for the award of the degree of
Master of Engineering (Electrical)

Faculty of Electrical Engineering
Universiti Teknologi Malaysia

FEBRUARY 2006

Especially for my family and friends……..

"Thank you for the understanding, my success is yours too"

ACKNOWLEDGEMENT

Thankfully, to Al-Mighty Allah SWT, I want to take this chance to acknowledge the contribution of several people who helped me to complete this thesis. I would like to express my appreciation and gratitude to my supervisor, Assoc. Prof. Dr. Ahmad Zuri Sha'ameri, for his guidance, support, and patience during my graduate education. He has been an invaluable source of technical knowledge and has certainly helped inspire many of the ideas expressed in this thesis. I had received great benefits from the graduate level courses on Advanced Digital Communication and also Digital Signal Processing which is taught by Dr. Ahmad Zuri Sha'ameri.

I would like to extend my gratitude to En. Jeffri Ismail, our DSP lab technician, for his technical assistance. I would also like to thank all the lab members who have made the lab a very happy environment to work in. Special thanks to the lab members who have helped me during the field-testing phase of my research.

I also would like to thank Mr. Wan Roz Wan Hussien from RF Communication Sdn. Bhd. for introducing me on HF and VHF communication system. With his guidance and technical support on KAM'98 HF modem, this project becomes successful.

Finally, special thanks go out to my family, for their patience, prayers, support and understanding over the entire period of my studies.

ABSTRACT

Nowadays, with the new technology development, communication is not limited by the distances, places and time. However, the infrastructures of communication still become an issue especially in the remote places. Therefore, this project focuses on long distance communication using radio frequency spectrum. High Frequency (HF) refers to the band from 3 to 30 MHz. This radio frequency spectrum allows the communication to be made for long distances either 100 km or more, direct by sky-wave propagation. By using existing HF radio and modem, a software application was developed to allow people to exchange their digital information in the form of short messages, text files and images. This system is suitable for the people at remote areas and sea where the communication infrastructure does not exist. In order to keep information secured while transmission, the system was incorporated with cipher algorithms. The block cipher AES (Advanced Encryption Standard) is used for authentication and key distribution while the stream cipher that is based on the linear feedback shift register (LFSR) is used for confidentiality. For that purpose, several stream ciphers algorithms such as shrinking, multiplexing and memory generator were analyzed to determine their characteristics. The analysis consists; statistical test, correlation attack, linear complexity profile and guess-and-determine attack which were done to verify the strength of ciphers. From the analysis, both Self-Shrinking and W7 generator succeeded all tests but, only W7 generator is adopted into the software application. Based on field-testing on designated sites, the system is user-friendly, reliable, secured, free error transmission and operates at low power of transmission.

ABSTRAK

Kini, dengan teknologi yang semakin membangun, perhubungan tidak lagi terbatas kepada faktor jarak, tempat dan waktu. Walaubagaimana pun, kemudahan komunikasi masih lagi menjadi isu terutama di kawasan-kawasan yang terpencil dan jauh dari bandar. Justeru itu, projek ini telah memberi penumpuan kepada perhubungan jarak jauh menggunakan frekuensi tinggi yang meliputi 3 hingga 30 Mega hetz sebagai medium perhubungan. Dengan menggunakan frekuensi ini, komunikasi boleh berlaku secara terus pada jarak 100 km atau lebih. Menggunakan radio dan modem yang sedia ada, sebuah perisian telah dibangunkan bagi membolehkan pengguna bertukar maklumat sama ada mesej pendek, fail teks mahupun gambar. Sistem ini adalah amat bersesuaian terutamanya bagi pengguna-pengguna di kawasan pedalaman dan juga di lautan yang tiada kemudahan perhubungan. Bagi memastikan maklumat yang dihantar adalah sulit dan selamat, sistem ini telah disertakan bersama dengan penyahkod. Penyahkod jenis blok iaitu AES (Advanced Encyption Standard) digunakan untuk pengesahan identiti dan penghantaran kunci rahsia manakala penyahkod jenis bit yang menggunakan anjakan semula daftar sebagai asas digunakan bagi memastikan maklumat adalah sulit. Bagi tujuan itu, beberapa jenis penyahkod jenis bit seperti *shrinking*, *multiplexing* dan *memory generator* dianalisis untuk mengetahui ciri-ciri penyahkod berkenaan agar kekuatan dan juga kelemahannya dapat ditentukan Analisis adalah berdasarkan ujian-ujian standard dan juga bukan standard. Daripada analisis, hanya penyahkod *Self-Shrinking and W7* lulus kesemua ujian tetapi hanya penyahkod W7 digunakan di dalam aplikasi sistem. Berdasarkan ujian lapangan yang telah dibuat, sistem ini memenuhi kesemua kriteria-kriteria untuk menjadi sistem komunikasi yang moden.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF SYMBOLS

a_i	-	Sequence of LFSR 0 or Register 0
b_i	-	Sequence of LFSR 1 or Register 1
$c(i)$	-	LFSR coefficient
$c_{in}(n)$	-	Carry-in
$c_{out}(n)$	-	Carry-out
$f(x)$	-	Polynomial over GF(2)
$g(x)$	-	Polynomial over GF(2)
k	-	Number of bits
L_N	-	Linear Complexity Profile
M	-	Number of LFSR
N	-	Number of bits in the sequence
N_c	-	LFSR stage
N_0	-	Number of 0's in a binary sequence
N_1	-	Number of 1's in a binary sequence
N_{00}	-	Number of transition of "00" in a binary sequence
N_{01}	-	Number of transition of "01" in a binary sequence
N_{10}	-	Number of transition of "10" in a binary sequence
N_{11}	-	Number of transition of "11" in a binary sequence
p_n	-	Period
R_n	-	Register
$R_{ss}(m)$	-	Autocorrelation Function
$s(n)$	-	Sequence of LFSR
χ^2	-	Chi-square
$z(n)$	-	Sequence of Keystream

LIST OF ABBREVIATIONS

AC	-	Alternating Current
AES	-	Advanced Encryption Standard
ALF	-	Absorption Limiting Frequency
AMTOR	-	Amateur Teleprinting Over Radio
AND	-	Logical AND
ARQ	-	Auto-Repeat Request
ASAPS	-	Advanced Stand Alone Prediction System
ASCII	-	American Standard Code for Information Interchange
CW	-	Morse Code
DES	-	Data Encryption Standard
DH	-	Diffie-Hellman
DSP	-	Digital Signal Processing
DSS	-	Digital Signature Standard
FEC	-	Forward Error Control
FIPS	-	Federal Information Processing Standards
FREQ-MGT	-	Frequency Management
FTP	-	File Transfer Protocol
GD	-	Guess-and-Determine
GF	-	Galois Field
GSM	-	Global System for Mobile Communication
GTOR	-	Golay Teleprinting Over Radio
GUI	-	Graphic User Interface
GWPS	-	Ground Wave Prediction System
HF	-	High Frequency
ISI	-	Inter Symbol Interference

JPEG	-	Joint Photographic Experts Group
LAN	-	Local Area Network
LFSR	-	Linear Feedback Shift Register
MAC	-	Message Authentication Code
MCMC	-	Malaysian Communications and Multimedia Commission
MFC	-	Microsoft Foundation Classes
MUF	-	Maximum Usable Frequency
NIST	-	National Institute of Standards and Technology
NSA	-	National Security Agency
OS	-	Operating System
OWF	-	Optimum Working Frequency
PACTOR	-	Packet Teleprinting Over Radio
PRNG	-	pseudorandom number generator
PTT	-	Push to Talk
RTTY	-	Radio Teletypewriter
SMTP	-	Simple Mail Transfer Protocol
SWR	-	Standing Wave Ratio
TNC	-	Terminal Node Controller
UT	-	Universal Time
UTM	-	Universiti Teknologi Malaysia
VHF	-	Very High Frequency
WL2K	-	Winlink 2000
XOR	-	Exclusive OR

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

High frequency (HF) radio has been used as wireless communication method for decades especially for beyond line of sight communications. The high frequency spectrum refers to the band of radio frequency spectrum from 3 to 30 MHz. By using the refractive properties of the ionosphere, it is possible to use these frequencies for long distance communications by sky-wave propagation. Despite the introduction of satellite services, the use of this medium has been undergoing resurgence over the last few years (NTIA-ITS, 1998). The most important benefit is providing communication over thousands of miles, as far away as the other side of the world. The second advantage is, HF free to use because the ionosphere is not own by anyone and equipment required is with minimal infrastructure. Therefore, the cost to setup a HF communication system is much cheaper as compared to other means of communication such as satellite (Abdullah *et al.*, 2003).

The HF radio's usage has been expanded and propagation problems were overcame by new technologies in digital communication and digital signal processing (NTIA-ITS, 1998; MIL-STD-188-141B, 1999). This enhances the reliability of communication in the HF spectrum. Besides voice and telegraphy, text, fax and images can be transmitted by using HF modem (SailMail, 2004; Cruiseemail, 2004; Harris Corporation, 2002). These new technologies permit computer-to-

computer communication. In communication either connection-oriented or wireless, security such as authentication and confidentiality is important due to the broadcast nature of HF communication. But unfortunately, most of the existing HF commercial systems such as Sail Mail, Cruise Mail and Winlink 2000 do not provide any features for authentication and confidentiality. Only products from Mils and Crypto AG (Mils, 2004; Crypto AG, 2004) promised that kind of security components. Others are only available as part of military communication equipment and is too costly for commercial user. Thus, the purpose of the research is to develop a HF Messaging System for commercial use that incorporates with security properties such as authentication and confidentiality.

1.1 Objective

The main objective of this research is to develop a messaging system that permits personal computers to exchange digital information such as short messaging, image transmission and text file over HF radio. This system is useful for places where terrestrial-based links are not possible or unreachable by land like ship or on an aircraft. Unlike existing systems that is based on military standard (FED-STD-1045A, 1994; MIL-STD-188-141B, 1999; Renfree, 2001), this system will cooperate with commercial modems and radios as a different building block of the system. This will ensure that the system is cheaper and available to application such as amateur radio operator, telemetry, diplomatic and shipping. In addition, the system will include authentication and confidentiality. This is important to ensure that the communication is confidential and not intercepted by unauthorized third party. For that purpose, the research also focuses on analyses of various types of stream cipher algorithms to determine their strengths and weaknesses. This can be performed based on standard and nonstandard test. By incorporating the best stream cipher into the HF messaging system, the communication link can be made practically secured.

1.2 Scope Of Study

This research scope is to develop a messaging system, which uses the HF communication channel as propagation medium. The system is developed by using Microsoft Visual C++ software and using Windows platform as Operating System. As part of the system, some ciphers are employed to ensure confidentiality and authentication in the data transmission between the terminals. The block cipher AES (Advanced Encryption Standard) is used for authentication and key distribution while the stream cipher that is based on the linear feedback shift register (LFSR) is used for confidentiality.

There are 2 types of stream cipher which produces keystream in bit or byte size. Shrinking, multiplexing and summation register (Menezes *et al.,* 1996) are examples of bit oriented while SNOW (Ekdahl, 2001), SOBER (Rose, 2000) and LILI-128 (Dawson, 2000) which produced keystream in byte size. In order to verify whether the stream cipher used is secured, some analyses are required to measure its strength. The analyses focus on stream ciphers that produces keystream which is bit oriented and based on 64 bits key. Basically, the strength of stream cipher correlates with the size of key used. Although the algorithms is not good but with the large key use and excellent key management scheme, its can increase their performance. Therefore, with the constant key length which is 64 bits, the strength comparisons of stream ciphers were made. Due to the system developed, the security is not limited to 64 bit key but can be enhanced by increasing the key length to 128 bits or more. This is because the key length can be extended by increasing the size of the LFSR.

The research does not involve designing or creating a HF modem, HF radio set or antenna. The frequencies that is used during transmission is determined using third party software called ASAPS (Advanced Stand Alone Prediction System) and also based on license given by MCMC (Malaysian Communications and Multimedia Commission). With the best usable frequency that counters from prediction, the

system will control the KAM'98 HF modem for data transmission. By including a suitable cipher algorithm the communications is practically secured.

1.3 Problem Statement

Computer networks normally transfer data via ground-based communication infrastructure such as telephone lines and fiber optic cables. However, this is impossible to communicate with places where terrestrial-based links are not possible and unreachable places by land such as on a ship, or on an aircraft. Satellite can be used but studies (Abdullah *et al.*, 2003) have shown that it is too costly. Thus, HF radio becomes the alternative communication medium for data transmission. Recently, when the tragic tsunami disaster happened in Aceh, all the communication systems were shut down. Therefore, the help from neighboring countries is found difficult. At that time, the only communication between them and the outside world is HF communication and this unexpected situation shows the significant of HF communication.

In general, the broadcast nature of any radio communication system such as HF communication makes it vulnerable to an unauthorized third party. Thus, there is a need for authentication, confidentiality and integrity services. This is to ensure the authorized users are using the system and to ensure the message is not access by unauthorized third party. Due to noisy channel and bulk transmission of data, stream ciphers are ideal choices over block ciphers based on faster implementation speed and do not introduce error of propagation. Hence, the research focuses on analysis and implements of the stream cipher algorithms to provide confidentiality. By employing the block and stream ciphers for authentication and encryption, the system will provide a secured messaging system over HF medium.

1.4 Research Methodology

In order to achieve the objective, the research approaches are as follows:

(i) Review on HF communication and related field in order to understand the basic concept and existing problem in HF transmission.

(ii) Review on cipher algorithms and available HF messaging systems also required for comparison and references.

(iii) Attends digital signal processing, digital communication and encryption course to enhance basic knowledge in the area of research.

(iv) The system design begins with the development of a messaging system using Visual C++. At earlier stage, both terminals are connected directly via serial link using RS232 cable.

(v) Then, designs a program to control HF modem. The program shall be capable to control basic functions for transmitting and receiving purposes.

(vi) Implement authentication procedure and session key generation using AES block cipher.

(vii) Analysis of stream ciphers for confidentiality. The analysis will be made based on standard and nonstandard test.

(viii) Field-testing of the system is conducted to verify the performance based on the Kuala Lumpur-Skudai HF link and other designated sites.

1.5 Thesis Outline

This thesis is divided into six chapters, including the current one. Chapter 2 presents the literature survey that was done at the earlier stage of the research such as ionosphere properties, HF communication, cryptography and current technology development in HF communications. It also contains about authentication and some key distribution technique in order to keep information secured.

Chapter 3 present the theory of stream cipher and block cipher algorithms including the basic model of stream cipher, examples of existing stream ciphers, statistical test, and others strength tests. It is also describing the example of polynomials and register setups that are used for analysis.

Chapter 4 explains the system designed and implementation. It is starting with system components, security features, radix 64 encoding, software implementation and several modifications that have been made during the implementation. Chapter 5 presents the analyses results of various types of stream cipher algorithms. Here, the best stream cipher is determined and adopted into the system. Then follow the experimental results, which are based on UTM Skudai and other designated sites.

Finally, Chapter 6 consists of the conclusion of works and contributions made in this thesis. It also includes future works that can be done further from this research.