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.