Cryptography in a Live Chat Application

by

Shon Verch

September 10, 2017

Cryptography in a Live Chat Application

by

Shon Verch

Abstract

This paper takes an in depth look into a variety of cryptography methods in order to determine their compatibility in a live chat application. The goal of encrypting data is to make it secure such that if the data is comprised, it is not at risk.

This paper also evaluates the security of different cryptography methods and their relation to a live chat application. A basic live chat application is built and applied to the various algorithms discussed within this paper. Comparisons of both theoretical and practical results are given in order to better understand the algorithms viability.

Contents

Chapter 1

Introduction

Cryptography has been rooted in some of history's most important conflicts. During World War 1, in January of 1917, British cryptanalysts deciphered a German telegram from the German Foreign Minister *Arthur Zimmermann* to the German Minister of Mexico *Heinrich von Eckardt*. The message was a proposition to Mexico, offering United States territory in return for joining the Central Powers.[1] On February 24th 1917, the British presented the telegram to President *Woodrow Wilson* of the United States of America. Shortly after, on April 6th, 1917, the United States of America officially declared war on the Central Powers [5]. The impact that cryptanalysis had on the war was tremendous forever changing the course of history. Not only had it caused the United States of America to enter the war but it also put cryptography in the forefront of political and military strategy.

The history of cryptography can be traced back to 4000 years ago in the Egyptian town of *Menat Khufu*. Hieroglyphics on the tomb of *Khnumhotep II* were written with unusual symbols such as to obfuscate the meaning [1].

The word *cryptography* derives from the Greek word ***kryptos*** meaning hidden and ***graphein*** meaning writing [4]. Cryptography is the science of concealing information in such a way that the message may only be read by whom it is intended for [3]. Likewise, *cryptanalysis* is the study of deciphering codes where the key is unknown [2].

A live chat application is a software which allows two or more users to communicate in real-time. Over the internet, the messages that are sent will typically be relayed by many other hosts outside of the control of the sender or recipient. Because of this, it is possible for data being transmitted over the network to be compromised by a third-party. To combat this, we can employ the use of cryptography to encrypt messages before being sent and then decrypt them upon delivery. This paper will examine different cryptography algorithms and how they work within a live chat application.

[1] The Central Powers were comprised of Germany, Austria-Hungary, the Ottoman Empire and Bulguria; also known as the *Quadruple Alliance* [6].

Chapter 2

Early Cryptography Methods

2.1 The Scytale

Bibliography

[1] *A Brief History of Cryptography*. 2013. URL: http://www.cypher.com.au/crypto_history.htm (visited on 09/10/2017).

[2] "Collins English Dictionary - Complete & Unabridged 10th Edition". In: (2017). URL: http://www.dictionary.com/browse/cryptanalysis (visited on 09/10/2017).

[3] "Dictionary.com Unabridged". In: (2017). URL: http://www.dictionary.com/browse/cryptography (visited on 09/10/2017).

[4] Monica Pawlan. *Cryptography: The Ancient Art of Secret Messages*. URL: http://www.pawlan.com/monica/articles/crypto/ (visited on 09/10/2017).

[5] *The Zimmermann Telegram*. URL: https://www.archives.gov/education/lessons/zimmermann (visited on 09/10/2017).

[6] Wikipedia. *Central Powers — Wikipedia, The Free Encyclopedia*. 2017. URL: https://en.wikipedia.org/w/index.php?title=Central_Powers&oldid=799418643 (visited on 09/10/2017).