Symmetric Key Cryptography

Connor MacNeil

Yohanes Hailegiorgis

Jordan Meade

Kevin Diez-Ocampo

Table of contents

Introduction

Symmetric Key Cryptography is a form of encryption that uses a secret key to encrypt and decrypt data. Our group chose this topic because encryption algorithms are the backbone of web security. This project is an opportunity to gain experience working with encryption algorithms, and gain an understanding of how they make it safer to communicate across the internet.

Problem description

The importance of encryption

Symmetric Key Cryptography addresses the critical need for securing sensitive information. Encryption algorithms, such as SKC, are essential in order to safely transmit information in a way that only authorized parties, i.e. the key holders, can access and interpret it. Many key technologies that we rely on a daily basis use cryptographic algorithms (e.g. WiFi).

Why is it necessary to encrypt information?

The internet is a particularly unsafe medium to transmit information because messages are very rarely transmitted directly from the source machine to the destination. In reality, information often goes through a multitude of routers and intermediaries before reaching its destination. This makes internet users and websites particularly vulnerable to man-in-the-middle attacks, where messages sent by a user to a website, or vice versa, are intercepted by a malicious node in the network.

Laws and Regulations concerning the confidentiality and integrity of data

In addition to the security concerns, web developers have a legal interest in securing their applications (via encryption and other means). In response to the growing concerns surrounding data security and privacy, governments around the world have enacted laws and established legal frameworks to ensure the confidentiality, integrity, and proper handling of sensitive information.

For instance, in the United States, laws such as the Health Insurance Portability and Accountability Act (HIPAA) [1] for the healthcare industry [], and the Gramm-Leach-Bliley Act (GLBA) for financial institutions [2], require organizations to implement specific security measures, including encryption, to protect sensitive data.

Similarly, in the European Union, the General Data Protection Regulation (GDPR) [3] sets out comprehensive rules for the protection of personal data []. It mandates that organizations implement appropriate technical and organizational measures, including encryption, to ensure the security of personal data.

How does it work?

Transmission of **plaintext** data poses a significant concern as it exposes information to potential interception. By using symmetric key cryptography, the body of a message is transformed into something illegible, called a **ciphertext**, before being transmitted. Only the holders of the secret key can easily decode the information within the message. Encryption can still be cracked by an attacker given enough time and resources; however, brute forcing an encryption key is computationally *very* expensive [4], which makes it impractical in most scenarios.

Solution description

Demo application

For our presentation, our team will develop a messaging application that allows two users to send messages back and forth. These messages will first be encrypted using an SKC algorithm, then transmitted to the server. Then the server will forward the message to its recipient, who can decode and read it. During our presentation we will disable the encryption on our application to show the audience the many ways in which an attacker can gather information from intercepted messages, and/or from a compromised server.

Work plan

Team member	Task	Est. time required
Report		
Connor	Solution description & results	8 h
Jordan	Lessons learned, overall experience & conclusion	8 h
Presentation		
Jordan	Presentation script	16 h
Jordan	Presentation slides & formatting	16 h
Solution: UI		
Kevin	Implement page layout and set-up boilerplate	TBD
Yohanes	Implement chat room selector	TBD
Connor	Implement chat box	TBD
Yohanes	Implement chat history	TBD
Solution: Backend		
Kevin	Determine best backend solution, set-up project boilerplate (project layout, repository, set cloud provider)	TBD
Kevin	Implement receive / send message endpoints	TBD

References

[1] Federal Trade Commission, *Gramm-Leach-Bliley Act*. 1999. Accessed: Jun. 22, 2023. [Online]. Available: https://www.govinfo.gov/content/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf

[2] *Health Insurance Portability and Accountability Act of 1996*. 1996. [Online]. Available: https://www.govinfo.gov/content/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf

[3] *General Data Protection Regulation*. 2016. Accessed: Jun. 22, 2023. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

[4] J. Fischer, "How much would it cost in U.S. dollars to brute-force a 256-bit key in a year?," *Cryptography Stack Exchange*. https://crypto.stackexchange.com/questions/1145/how-much-would-it-cost-in-u-s-dollars-to-brute-force-a-256-bit-key-in-a-year/1147#1147 (accessed Jun. 22, 2023).