Cryptography and Networks

Saint Leo University

COM 450- Network Defense and Security

Instructor: Dr. Omar

Shane Irons

March 24, 2020

Abstract

This paper will look at Cryptography related to Network Security and some techniques commonly used within this parameter. With some background knowledge about the fundamentals of Cryptography, we will go more in-depth about its importance, modern uses, and some standards while still relating to network security.

1.0 Introduction

Cryptography, put simply, “is the study and practice of techniques for secure communication in the presence of third parties.” **[1]** For example, encryption is a common form of Cryptography used in Network Security. Allowing the desired party to view the data without compromise/interference from unwanted or unknown parties is the basis of this discipline.

2.0 Background

Regarding Network Security, Cryptography is implemented to ensure secure communication, whether between two users, two networks, two servers, etc. If data is being sent from one place to another, then there is a possibility someone with malicious intent is looking to intercept it. The roots of Cryptography date back to Roman and Egyptian civilizations, as referenced by the popular method of Cryptography named the “Caesar Shift Cipher”. Later famous instances of Cryptography involve the Vigenere cipher, implementing a series of Caesar ciphers, and the Enigma cipher, used by Germans implementing machinery in World War II. To maintain secure transfers of information, Cryptography is often implemented.

3.0 Importance of Cryptography

Regarding Network Security, data being transferred should look to adhere to the CIA triad, as depicted in **Figure 1:**

Figure 1: *CIA Triad Model for Information Security*

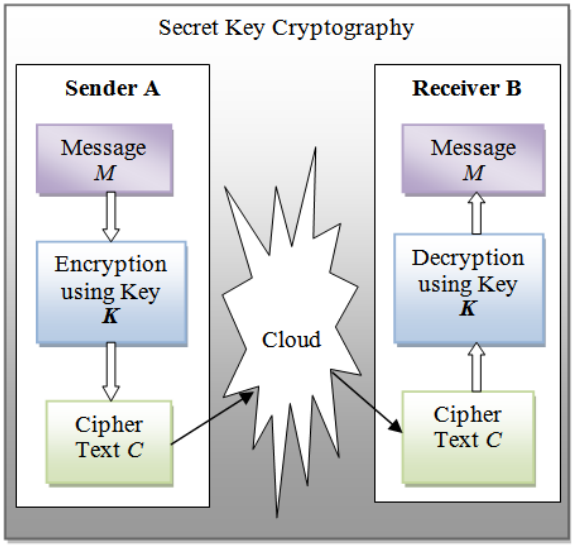
The main components of the triad including Confidentiality, Integrity, and Availability, as well as Non-repudiation are the core disciplines of Information Security, overlapping with Cryptography. To Network Security, encrypting data that is transferred across a network should be a feature implemented by the network administrator in the form of protocols and firewalls. Common protocols include TLS/SSL, IPsec, and SSH. Without protections set by the administrator, the network becomes untrustworthy as data may be stolen or users may be compromised.

4.0 Modern Use of Cryptography

The modern use of Cryptography is done in one of three ways: secret key (symmetric), public-key (asymmetric), and hash functions **[2]**.

4.1 Symmetric Encryption

With single key (aka symmetric encryption) Cryptography, only one key is used in both the encryption and decryption process **[2]**.



With this type of encryption, the cipher's categorized as being either stream or block. Stream ciphers operate bit by bit and block ciphers operate with blocks of data at a time **[2].** With this form of cryptography, both parties must know the key, so distribution of a key is done discretely with minimal parties involved.

Figure 2: *Secret Key Cryptography* ***[2]***

For reference, some common modern Symmetric Encryption algorithms include: Data Encryption Standard (DES), Advanced Encryption Standard (AES), Blowfish, Twofish, Camellia, and Kasumi **[2]**.

4.2 Asymmetric Encryption

Put simply, Asymmetric Encryption often uses two keys (public and private), one to encrypt and the other to decrypt **[3]**, also depicted in **Figure 3**.

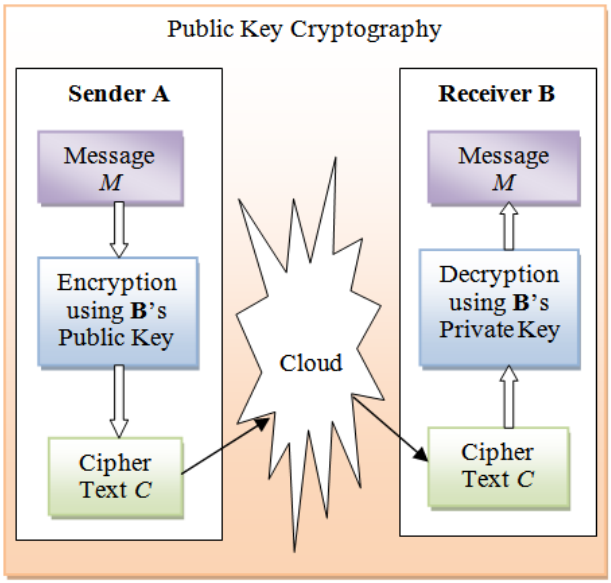


Figure 3: *Public Key Cryptography* ***[2]***

Public Key Cryptography (aka Asymmetric Encryption) using the typical key exchange (or digital signature) approach utilize a few different algorithms: RSA, Diffie-Hellman Key Exchange, Elliptic Curve Cryptography, and Digital Signature Standard **[2]**. Since multiple keys are used, this defeats a single point of failure, and an adversary must break 2 (or more) keys to crack the encryption; Multiple keys and stronger security make Asymmetric Encryption lean heavier toward the Confidentiality and Authentication aspects of Network Security **[2]**. Although more confusing due to the number of keys and setup required, the communication system becomes much more secure **[3]**.

4.3 Hash Functions

These functions are essentially formulas that encrypt data without a key. The focus of hash functions is to maintain data integrity **[2]**. Utilizing compression, these encryption methods are mathematical functions converting any inputted value into a numerical value **[4]**. The length of the input data is random, but the output is fixed in length **[4]**.

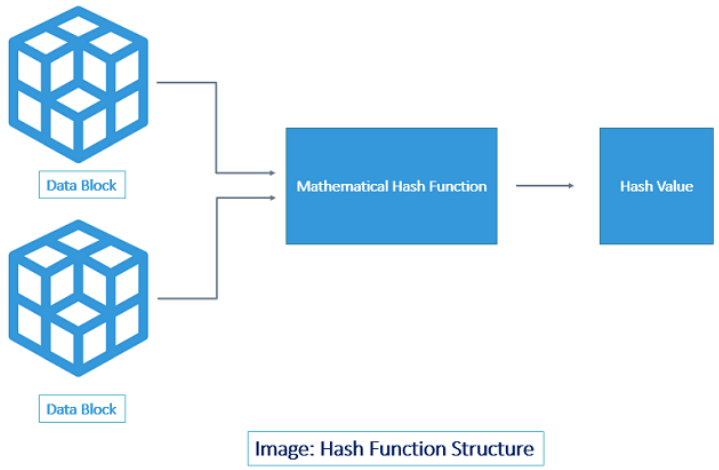


Figure 4: *Hash Function Structure Simple* ***[4]***

In **Figure 4**, it is shown simply with data blocks being inserted into a "Mathematical Hash Function", which outputs a hash value. This is a simple illustration, and as seen, no keys are typically used. A group of these functions fall under a family called the Secure Hash Algorithm (SHA) which can take in varying sizes of messages, block sizes, and utilize varying steps in the mathematics **[2]**.

5.0 Standards

In Cryptography, standards are used to ensure uniform levels of encryption across network users. These are important specifications since to become a standard, a security protocol must: be stable/well understood, be competent, have multiple interoperable implementations, have public support, and be recognized as useful **[5]**. The Internet Engineering Task Force (IETF) is the organization that recommends specifications through a series of Request for Comments (RFC) to the Internet Engineering Steering Group (IESG), who ultimately decides which RFCs become internet standards **[5]**. Some common network security standards from the IETF that implement cryptography include: Kerberos (secret key authentication), IPsec (provide

data CIA [**Figure 1**]), X.509 (public key verification), S/MIME (public key encryption), and TLS (symmetric encryption providing data integrity) **[5]**. Of course, many regulations are in place to ensure high quality processes become standards that are implemented across networks and the internet.

Conclusion

In conclusion, understand that Cryptography refers to protecting information using codes, typically by encoding and decoding blocks of data. Understand there are multiple ways of using Cryptography to the advantage of Network Security and practitioners should be aware and often implement the most current standards. Cryptography is not a perfect solution, it is only a part of the whole picture, and other practices in Network Security should not be overlooked.

References

- **[1].** Cryptography Introduction. (2020, February 13). Retrieved from https://www.geeksforgeeks.org/cryptography-introduction/
- **[2].** Kumar, S. N. (2015, January 23). Review on Network Security and Cryptography. Retrieved March 24, 2020, from http://pubs.sciepub.com/iteces/3/1/1/index.html#
- **[3].** Cryptography and Network Security. (n.d.). Retrieved from https://www.ecpi.edu/blog/crypotgraphy-and-network-security
- **[4].** Gajjar, M. (2019, October 4). Decoded: Examples of How Hashing Algorithms Work. Retrieved from https://cheapsslsecurity.com/blog/decoded-examples-of-how-hashing-algorithms-work/
- **[5].** Stallings, W. (2019). *Cryptography and network security: principles and practice*.