Tittle

Comparison of Cryptographic Methods

& Key Exchange

Ayodele Esho

Student ID: 201499108

Contents

[Abstract 1](#_Toc101717687)

[Introduction 1](#_Toc101717688)

[Secrete Key Cryptography 2](#_Toc101717689)

[Asymmetric Encryption 2](#_Toc101717690)

[Hashing 2](#_Toc101717691)

[Key exchanges 2](#_Toc101717692)

[D-H Key Exchange method 2](#_Toc101717693)

[RSA key exchange method 3](#_Toc101717694)

[Comparison 3](#_Toc101717695)

[Reference 3](#_Toc101717696)

## Abstract

Cryptography is a collection of mathematical techniques for protecting information. Encryption/decryption is the most significant cryptographic procedure. It can be used in a variety of applications, including: email, file sharing, and secure communication. Cryptography can also be used to protect digital data such as emails, files and messages. The digital age has enhanced the importance of cryptography in recent years. Cryptography originally originated with ciphers, the first algorithm was called ‘Caesar Cipher’. At the time ciphers were easier to decipher than the present day cryptography algorithms. Over the years Cryptography has developed more advanced methods due to its need for data to be more protected and more secure.

## Introduction

Cryptography can be separated into 3 main categories. Which are:

* Secrete Key Cryptography
* Public Key Cryptography (Asymmetric Encryption)
* Hash functions

## Secrete Key Cryptography

Secrete Key cryptography (also known as symmetric cryptography) contains a single key used to encrypt and decrypt data. The system is used to encrypt the plaintext message using a series bits known as the secrete key. It uses the same key to decipher the ciphertext message and retrieve the original plaintext. Both encryption and decryption is accomplished with the same key. However, an asymmetric encryption, is known as a public-key cryptography. The key encrypts and decrypts data with two different keys. The keys are known as a private and public key. The public key is used for encryption and, the private key is used for decryption. A prime example of this is:

Plain text -> Encryption Algorithm -> Ciphertext -> Decryption Algorithm -> Plaintext

This means that one party sends a message transformed from its plaintext into its encrypted ciphertext and the other side reverses it to its original message form.

The symmetric encryption is faster, however the downfall of it is that if the key falls into the hands of a user’s with malicious intentions, they will have the opportunity to be able to decrypt that message and read the content that it contains. For security, a symmetric encryption depends on the secrecy of the key and not the secrecy of the algorithm. The reason for this is because it is difficult to invent new algorithms and keep them a secrete, and producing keys is a lot easier.

Symmetric encryption algorithms uses algorithms such as; 3DES and AES. 3DES (Triple Data Encryption Standard) was an algorithm created to protect against brute force attacks. 3DES is an updated version of DES. Once DES weaknesses were unrevealed 3DES was made. The difference between DES and 3DES, is that the key size is tripled to provide extra security, for total key length of 168 bits. This means that 3DES encrypts the inputted data three times. AES (Advanced Encryption Standard) algorithm is a block cipher but converts individual blocks using keys of 128,192 and 256 bits. The ciphertext is formed by combining them once they are encrypted. The way we known AES is a symmetric algorithm, is that it uses the same 128, 192, or 256 bit key for both encryption and decryption.

## Asymmetric Encryption

In comparison with asymmetric encryption uses two keys. So that If the users is able to achieve the public key it will also need the private key to decrypt the message. However is required to use large amounts of computing power. Common asymmetric algorithms are: RSA, ECC, DSA.

## Hashing

Another Cryptography function is Hashing. Hashing, is the act that converts a set of strings into another set of unreadable strings of characters. The function was created to complexify data, prevented it to be read by all parties. Most good hash functions uses a one way algorithm, making it harder for hackers to reverse engineer the data. To further the complexity, users often use the technique salting, which adds another value to the original set of hashed characters. Hashing is often used for passwords.

## Key exchanges

Key exchange, is the method in cryptography that is used to exchange cryptographic keys between two different parties. During the process of the key exchange, each party sends their public key to one another, that key is then used and shared secretly to generate a new private key for communication. If either parties (sender & receiver) desires to send encrypted messages to one another, they must be both able to encrypt and decrypt messages. The keys can also be used with an symmetric key algorithm to pass data in a protected way. The symmetric algorithm Is used to encrypt the large portion of the data. There a number of methods to exchange keys.

## Methodology

One method is the Diffie-Hellmann key exchange method. The method was created by Whitfield Diffie and Martin Hellmann in 1976. The system works by using two difficult mathematical problems: one easy to solve but slow to solve; the other hard to solve but fast to check. Both parties uses the mathematical algorithm and generate a shared secrete Key, which is then used to share encrypted information. There are also other Key Exchange methods such as; RSA key exchange. RSA key exchange was developed in 1978 by Ron Rivest, Adi Shamir and Leonard Adlemanin. RSA is used to transmit data between multiple parties through a secure channel. RSA uses a combination of public keys and private keys, known as a asymmetric cryptography. However even thought the public key is shared the private key is kept secret.

## Comparison

The difference between RSA and DH key exchange is that RSA uses a trapdoor function and DH relies on Discrete Logarithm. RSA can be used for encryption and signature generation and DH is used for key agreement which be used for encryption or authentication. RSA algorithm is more commonly used as its more secure against cyber-attacks, where as the DH key exchange method is open to attacks known as ‘man-in-the-middle’.

# References

Anon., n.d. *Wikipedia.* [Online]   
Available at: https://en.wikipedia.org/wiki/Key\_exchange

Franklin, R., March 13, 2021. [Online]   
Available at: AES vs. RSA Encryption: What Are the Differences? (precisely.com)

GeeksForGeeks, 29 Jan, 2020. [Online]   
Available at: https://www.geeksforgeeks.org/difference-between-private-key-and-public-key/

Glossary, G., n.d. [Online]   
Available at: https://www.gartner.com/en/information-technology/glossary/secret-key-cryptography

Hyper, 2022. [Online]   
Available at: https://www.hypr.com/secret-key/

Lake, J., March 23, 2021. [Online]   
Available at: https://www.comparitech.com/blog/information-security/diffie-hellman-key-exchange/

Matthews, T., September 03, 2019. [Online]   
Available at: https://www.exabeam.com/information-security/rsa-algorithm/

Millett, L. I., n.d. [Online]   
Available at: http://www.cs.cornell.edu/courses/cs513/2004SP/L24.html

Ohri, A., 5 Jan 2021. [Online]   
Available at: https://www.jigsawacademy.com/blogs/cyber-security/secret-key-cryptography/

Point, J., n.d. [Online]   
Available at: https://www.javatpoint.com/public-key-vs-private-key

Techopedia, n.d. [Online]   
Available at: https://www.techopedia.com/definition/16085/diffie-hellman-key-exchange