# Introduction

Cryptography highlights an aspect of secure programming and digital security. Cryptography provides the methods and techniques to protect data from unauthorized access and manipulation. Through advanced algorithms and encryption methods, data is transformed into a form that is inaccessible to outsiders, thereby ensuring confidentiality and integrity. This chapter describes the history and various approaches to encryption.

Cryptography is a secure communication technique that ensures only the sender, and the recipient of a message can view its contents. It involves a form of encryption where plain text is converted into what is known as cipher text and is then decoded upon receipt. This is done using a shared ‘key’ to decrypt the message. The message can contain anything from a simple WhatsApp message to highly sensitive government or banking data. The reason cryptography is used is that a hacker can eavesdrop on a connection between you as a user and, for example, a website. To prevent the transmitted information from being leaked, cryptography is used (Kaspersky, 2022).

When transmitting data, it is most common to use cryptography for encoding and decoding emails, login credentials, and other messages. One method involves symmetric cryptography, where data is encoded using a secret key, and both the encrypted message and the secret key are then sent to the recipient for decryption, as illustrated in Figure 1. The problem arises when the message is intercepted, as a third party then has everything needed to decrypt and read the message.

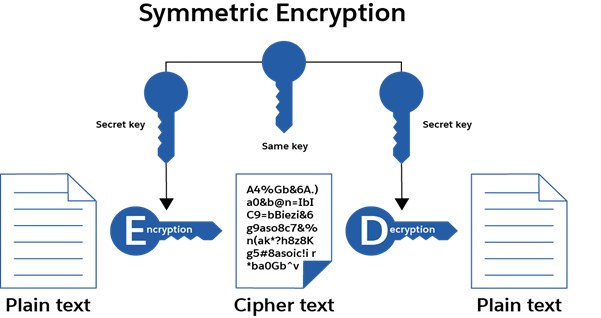


Figure : Encryption (Kavanagh, 2022)

# History

The concept of cryptography has ancient origins, with the earliest known form dating back to approximately 1900 BCE during Egypt's Old Kingdom. At that time, Egyptians employed non-standard hieroglyphs as a rudimentary encryption method. These hieroglyphs, shown in Figure 2, served not only as a form of communication but also as a method to obscure messages. Only scribes in service to the Egyptian pharaohs could interpret these messages, indicating an early understanding of restricted access to information (Guraseessingh, 2022).

****

Figure : Egyptian Hieroglyphs (Origin of Cryptography, n.d.)

Shortly after, the ancient Greeks introduced a more structured method of encryption: the **Caesar Cipher**, also known as the **Shift Cipher**. This technique involves substituting each letter in the plaintext with another letter from the alphabet, shifted by a specific number of positions. This simple substitution method renders the original text unreadable to unauthorized parties and requires a shared key for decryption. The shared key specifies the number of positions each letter is shifted (Guraseessingh, 2022).

Later, during the 16th century, the Vigenère Cipher was introduced by Blaise de Vigenère. It was originally devised in 1553 by Giovan Battista Bellaso but became widely known through Vigenère. It is a cryptographic technique where the key is repeated multiple times across the entire message. The ciphertext is then generated using a *tabula recta*, which is a matrix filled with alphabets. By allowing the letter from the message and the letter from the key to meet on the *tabula recta*, a new letter is produced. Repeating this process for each letter in the message results in a ciphertext (Guraseessingh, 2022).

**A blue squares with black letters

AI-generated content may be incorrect.**

Figure : Vigenère Cipher (thesecuritybuddy)

Subsequently, in the early 19th century, Edward Hugh Hebern invented the Hebern rotor machine. This was a typewriter that used a special rotating disk. This disk functioned as a substitution alphabet, and the message was encrypted as you typed, as shown in Figure 4. The disk had a starting position, and by sharing this start position, the recipient could type the encrypted message backward on their own machine and get the decrypted message (Guraseessingh, 2022)

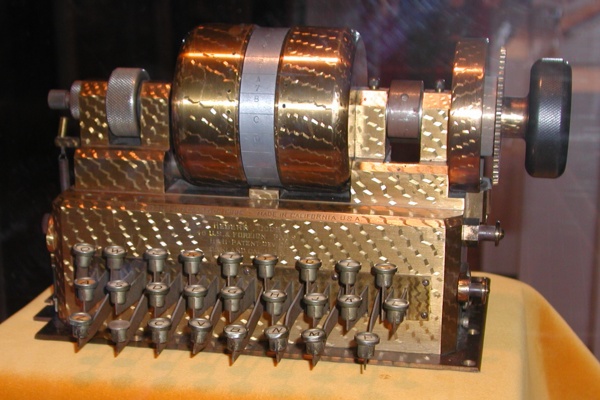


Figure : Hebern rotor machine (Guraseessingh, 2022)

It was one of the first "rotor machines" to be used as a primary form of cryptography during World War II. After World War I, the Germans developed their own rotor machine—the Enigma machine, as shown in Figure 5. The first model was invented by Arthur Scherbius and was later adopted by Nazi Germany for military use. Unlike the Hebern rotor machine, which had only one disk, the Enigma used 3 to 5 rotors. This made the encryption process significantly more complex, as it involved multiple shifting substitution alphabets. If the recipient had their machine configured in the same way as the sender, they could decrypt the message (Guraseessingh, 2022).

****

Figure : Enigma machine (History of the Enigma, 2012)

Today, there are many ways to apply cryptographic techniques. These include encryption, hashing, and signing. Encryption is a technique in which information is converted into ciphertext so that only users with authorization can access the decrypted text. Encryption often makes use of hashing, a technique that transforms text into unreadable characters. Lastly, there's the concept of signing, a technique used to verify that a message or information genuinely came from the sender and wasn't altered before reaching the recipient.

Cryptographic Algorithms  
Algorithms are mathematical formulas used to encode or decode data. They encrypt information so that only users with the correct key can access it. Algorithms can be used to secure personal data, bank information, or even a simple WhatsApp message. The types of algorithms that will be discussed are asymmetric, symmetric, and hash algorithms (Liska, 2016).

## Asymmetric Cryptography

Cryptographers devised a solution known as asymmetric cryptography. In this method, each user has two keys: a public key and a private key. Senders request the recipient’s public key, use it to encrypt the message, and then send the encrypted data. When the message arrives, only the recipient's private key can decrypt it. This means that theft is pointless without the corresponding private key (Synopsys, n.d.).

## Symmetric Cryptography

Symmetric cryptography is generally faster for encrypting large volumes of data, such as databases. Asymmetric cryptography is slower and can only encrypt data smaller than the 256-bit key size. Therefore, asymmetric cryptography is often used to encrypt symmetric encryption keys, which are then used to encrypt much larger blocks of data. For digital signatures, asymmetric cryptography is typically used (Synopsys, n.d.).

Some examples of symmetric encryption algorithms include:

* **AES (Advanced Encryption Standard)**
* **DES (Data Encryption Standard)**
* **IDEA (International Data Encryption Algorithm)**
* **Blowfish (drop-in replacement for DES or IDEA)**
* **RC4 (Rivest Cipher 4)**
* **RC5 (Rivest Cipher 5)**
* **RC6 (Rivest Cipher 6)** (Smirnoff & Turner, 2023)

## Hash Algorithm

A hashing algorithm is a method used to securely store and verify data. The hashing process involves converting an arbitrary amount of data (such as a password) into a fixed, unique code that is difficult to guess. This is done by passing the data through an algorithm that converts it into a hash value. This hash value can then be stored in a database or used to verify the authenticity of the data.

An important feature of hashing is that the process is irreversible. This means it is not possible to retrieve the original data from the hash value. This makes hashing a secure way to store and verify data because it prevents attackers from accessing the original information.

There are various hash algorithms available, such as **MD5**, **SHA-1**, **SHA-256**, and **SHA-512**. Some older algorithms, such as MD5 and SHA-1, are no longer considered secure for modern applications. Choosing a robust, secure hashing method is critical for resisting attacks such as brute-force or collision attacks (What Is a Hashing Algorithm? A Look at Hash Functions, 2023).

# Application of Cryptography in the Developed App

Certificate Pinning

Certificate pinning is a security technique used to ensure that an application communicates only with a trusted server that presents a specific SSL certificate. This method is particularly effective in preventing Man-in-the-Middle (MitM) attacks, in which an attacker intercepts and potentially manipulates communication between the app and the server.

In the developed application, SSL certificate validation occurs during the SSL handshake. If the presented certificate matches the expected certificate, the connection is considered secure, and data exchange is permitted. If the certificates do not match, the connection is terminated, and the application will not proceed with communication (Pandey, 2021).

In addition to certificate pinning, HTTPS is a fundamental aspect of secure communication in Android applications. HTTPS is a secure version of HTTP that encrypts data transmitted between the application and the server. This encryption protects sensitive information, such as login credentials, from being intercepted by malicious parties.

To implement HTTPS in an Android application, the app must connect to a server that has a valid SSL certificate installed. The app initiates a secure connection, which is verified against the server's certificate. If the certificate is valid, the app establishes a secure HTTPS connection with the server.

# Bibliography

Guraseessingh. (2022, Oktober 6). *History of Cryptography*. From GeeksforGeeks: https://www.geeksforgeeks.org/history-of-cryptography/

*History of the Enigma*. (2012, 3 12). From cryptomuseum.com: https://www.cryptomuseum.com/crypto/enigma/hist.htm

Kaspersky. (2022, Februari 9). *Cryptography Definition*. From Kaspersky.com: https://www.kaspersky.com/resource-center/definitions/what-is-cryptography

Kavanagh, A. (2022, 10 17). *SalesForce*. From security.salesforce.com: https://security.salesforce.com/blog/cryptography-everything-you-never-wanted-to-know

Liska, A. (2016). *Science Direct*. From sciencedirect.com: https://www.sciencedirect.com/topics/computer-science/modern-cryptography

*Origin of Cryptography*. (n.d.). From tutorialspoint.com: https://www.tutorialspoint.com/cryptography/origin\_of\_cryptography.htm#

Pandey, A. (2021, December 14). *SSL Pinning in Android - Apurv Pandey - Medium*. From Medium: https://mailapurvpandey.medium.com/ssl-pinning-in-android-90dddfa3e051

Smirnoff, P., & Turner, D. M. (2023, Maart 14). *Symmetric Key Encryption - why, where and how it’s used in banking*. From Cryptomathic: https://www.cryptomathic.com/news-events/blog/symmetric-key-encryption-why-where-and-how-its-used-in-banking

Synopsys. (n.d.). *What Is Cryptography and How Does It Work*. From Synopsys.com: https://www.synopsys.com/glossary/what-is-cryptography.html

*What Is a Hashing Algorithm? A Look at Hash Functions*. (2023, Februari 15). From Code Signing Store: https://codesigningstore.com/what-is-hashing-algorithm-how-it-works