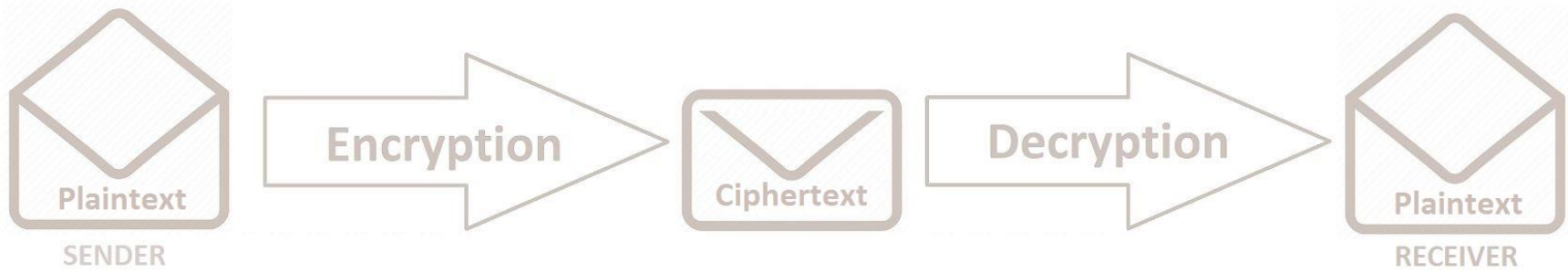
WRITTEN BY: HEIDI

Cryptography: Encryption vs. Decryption



Cryptography is an essential technique in cybersecurity, it is used to secure data confidentiality and preserve the originality of the contents or message between a sender a receiver. Cryptography is processed through encryption by the sender and decryption by the receiver. **Encryption** is the process of transforming an original message, known as 'plaintext', into an unrecognizable, non-readable or difficult to interpret format. This newly formatted message is known as a 'ciphertext'. **Decryption** is the process of transforming this encrypted message – 'ciphertext' – back to its original readable, recognizable format – 'plaintext'.

The selection method of encryption and decryption uses one of two types of encryption key algorithms:

Symmetric Encryption Algorithm – uses the same key for both encryption and decryption (This algorithm is also known as Private Key Encryption).

Asymmetric Encryption Algorithm – uses a public and private key for encryption and decryption. If a public key is used for encryption, the private key will then be used for decryption. Vice versa, if a private key is used for encryption the public key will then be used for decryption (This algorithm is also known as Public Key Encryption).

Public key – a key that is shared to the public, known to all parties.

Private key – a key that is only known to one party.

Caesar Cipher is a famous symmetric encryption algorithm; it essentially encrypts a message by shifting each character in the message by a number in the alphabetical sequence. For example, if the message to be encrypted is: "Today", by using a shift of 3 for each character the encrypted message is now: "Wrgdb". To decrypt this message, the receiver will have to make the same shift of 3 in the opposite direction for each character to revert back to the original message: "Today".

WRITTEN BY: HEIDI

Rivest-Shamir-Adleman (RCA) is an asymmetric encryption algorithm. This algorithm generates a public and private key linked to each other but not derivable from one another. The public key is used for encryption and the private key is used for decryption. An analogy to illustrate this would be using a physical address as a public key. The address is known to multiple parties (this could be friends, family, neighbors etc.) so if someone wanted to send a message (or mail in this case) to the resident of that address, the only person or party that will be able to read this message would be someone with the key to the mailbox at this address – hence the private key.

Symmetric encryption algorithms are usually fast to implement since they only rely on one public key, though this will require all individuals of the party to keep this public key private to those not involved. This however when scaled to a business perspective would be seen as a weakness as the reliant is heavily held on this one public key.

Asymmetric encryption, contrary to symmetric encryption will take a longer time to implement as it will have to generate a public and private key. This is more widely used in places where security really matters. The use of a public key for encryption and a private key for decryption ensures in verifying the target user that is decrypting the message. In a similar sense, the use of a private key for encryption and a public key for decryption guarantees that the message came from a specific user or source.

WRITTEN BY: HEIDI

References:

Security Team, “Public Keys and Private Keys in Public Key Cryptography”, *Sectigo,* Sectigo, 9 June 2020, https://sectigo.com/resource-library/public-key-vs-private-key

“Asymmetric Encryption”, *Teach Computer Science,* Teach Computer Science, https://teachcomputerscience.com/asymmetric-encryption/

“Encryption vs Decryption”, *EDUCBA,* EDUCBA, https://www.educba.com/encryption-vs-decryption/

Jörg, Kastning “Basic Concepts of Encryption in Cryptography”, *RedHat,* RedHat, Inc., 11 February 2021, https://www.redhat.com/sysadmin/basic-concepts-encryption-cryptography

“How does Public Key Encryption Work? | Public Key Cryptography and SSL”, *Cloudflare,* Cloudflare, Inc. https://www.cloudflare.com/learning/ssl/how-does-public-key-encryption-work/