Encryption Types: Symmetric and Asymmetric

University of the Cumberlands

Dr. Lori Farr

Jacob Jeffers

ISOL 535 – Cryptography

6/8/2021

**Abstract**

In this paper, I will analyze asymmetric and symmetric encryption, evaluate the differences between the two of them, and determine which is the most secure.

**Encryption Types: Symmetric and Asymmetric**

According to Diffie (n.d.). “Without strong encryption, you will be spied on systematically by lots of people.” Encryption is the process of taking cleartext and converting it into an unreadable form of text called ciphertext (Stallings, 2018). The purpose of this is to protect information at rest, in use, or transit (Johansen, 2020). Encryption promotes confidentiality, and it is the most secure way to store or send information (Stallings, 2018).

**Symmetric Encryption**

Symmetric encryption is also called “single-key encryption,” It is the most widely used encryption type; it works by utilizing a single key for encrypting and decrypting data (Stallings, 2018). Suppose Bob wants to send an encrypted file to Susan. Bob begins the process by taking the plaintext file and converting it into a ciphertext file using an encryption key. After this, Bob sends the file to Susan. To access the file, Susan needs the same essential Bob used for encryption to decrypt. After decryption, Susan is now able to see the file.

There are some things to consider. The algorithm used to encrypt and decrypt the data must be strong to prevent brute-force attacks on the file. This helps to ensure confidentiality and promotes security (Stallings, 2018). Another consideration is ensuring the secret key is not compromised in transit. Key distribution was a significant concern with symmetric encryption and made digital signatures impractical at the time (Stallings, 2018).

**Asymmetric Encryption**

Before the invention of the public-key infrastructure (PKI) in the 1970s, single-key encryption was the only used type (Stallings, 2018). The PKI was an evolvement of symmetric encryption which sought to answer two issues with symmetric encryption. The first was to answer crucial distribution; the second sought to make digital signatures more practical (Stallings, 2018). Asymmetric encryption utilizes two keys: one for encryption and one for decryption. These are often called the public key and the private key (Stallings, 2018). Using asymmetric encryption, suppose Bob wants to send Susan a file. Both parties would need two keys. The public key for each would be placed in a registry accessible for both. Bob wants to send Susan an encrypted file to encrypt the file, and Bob would do so using Susan’s public key. Bob then sends the encrypted file to Susan, and she decrypts the file using her private key. If Susan wanted to send a file back, she would use Bob’s public key, and Bob would decrypt the file with his private key. Key distribution is now solved because the private keys are never shared, and the public keys are saved to a virtual key ring that can be used to encrypt files as needed for the chosen recipient (Stallings, 2018).

**What is the Difference? Which is More Secure?**

There are some notable differences. Although symmetric encryption is still the most widely used, it is the older method when compared to asymmetric encryption. Symmetric or single-key encryption is the most widely used because it uses less computational power but still provides decent security (Cyware, 2020). Symmetric encryption utilizes a single key for encryption and decryption while asymmetric encryption uses one for encryption and one for decryption (Stallings, 2018). This means that asymmetric encryption is the more secure encryption type. However, it can be costly to implement (Cyware, 2020).

**Conclusion**

From an organizational standpoint, security should be one of the top priorities. Encryption is a way of ensuring that the data within the organization remains confidential. There are two main types of encryptions: symmetric and asymmetric. Symmetric encryption is faster, older, and more widely used. Asymmetric encryption is slower but newer and more secure. From a security perspective with an unlimited budget, the organization should be using asymmetric encryption. However, most executives use both types of encryptions for different use cases (Cyware, 2020).

**References**

Cyware. (2020, February 22). *Exploring the Differences Between Symmetric and Asymmetric Encryption: Cyware Hacker News*. <https://cyware.com/news/exploring-the-differences-between-symmetric-and-asymmetric-encryption-8de86e8a>.

Diffie, W. (n.d.). *Encryption Quotes*. BrainyQuote. <https://www.brainyquote.com/topics/encryption-quotes>.

Johansen, A. G. (2020, July 24). *What is encryption, and how does it protect your data?* Norton. <https://us.norton.com/internetsecurity-privacy-what-is-encryption.html>.

Stallings, W. (2018). *Cryptography and network security: Principles and practice*. Boston: Pearson Prentice Hall.