3-2 Journal: Cryptography

Joshua Merren

Southern New Hampshire University

CYB-250-11621-M01 Cyber Defense

Professor Tchinda Mbuna

15 July 2024

Cryptography forms an essential defense tool in cybersecurity, serving as the primary method for securing data by converting it from a readable format (plain text) into an encoded version (cipher text) that is only decipherable with a specific key. Plain text refers to any easily understandable data without decryption, including everything from text in an email to data stored on a corporate server. When encrypting data, a cryptographic algorithm and a secret key transform it, resulting in ciphertext. This cipher text appears as a random string of characters, incomprehensible without the appropriate decryption key. The secret key used during this process is crucial; it acts as the cipher's parameter that varies with each encryption session, ensuring that the resulting cipher texts are distinctly different even if the same data is encrypted multiple times. This variability is critical for securing data transmissions across networks where intercepts are possible, as it prevents unauthorized entities from making sense of intercepted data without the corresponding key.

In the realm of encryption, the methods employed can broadly be categorized into symmetric and asymmetric encryption, each serving distinct security needs dictated by their operational environments. Symmetric encryption uses a single key for encryption and decryption processes. This method is efficient, consumes less processing power, and enables faster data handling. It makes it ideal for encrypting large volumes of data or for use in systems where data frequently needs to be encrypted and decrypted. However, the major challenge lies in the secure exchange of the encryption key. To decrypt the message, both parties must share the same key securely to prevent interception. On the other hand, asymmetric encryption uses a pair of related keys—one public key for encryption and one private key for decryption. This essential pair approach eliminates the need to securely share keys in advance, as the public key can be distributed openly without compromising security. The private key is kept secret and used only by the recipient to decrypt the message. While this method offers enhanced security by facilitating safe key distribution, it is computationally more demanding and inherently slower than symmetric encryption, making it less suitable for some real-time applications or large-scale data encryptions.