Unit 7 Cryptography Concepts

**Corey Crooks**

**Purdue University Global**

**IT484—Cybersecurity Policies**

**Preston Rich**

**January 31, 2023**

**Part 1**

Throughout all cybersecurity disciplines, a need for privacy is perfect. Who has access to any given information, and when, may prove vital for the security and longevity of an organization and those that interacts with. Too secure these conversations come up many different disciplines have been developed. Chief among them, would be that of cryptography. Cryptography essentially turns a chunk of data into a puzzle to be unwound and solved at a later time. Just start the exchange, information is jumbled in a specific way according to a private key. Using either asymmetric or symmetric cryptography methods the receiving sight is then able to decrypt the information from the original package into plain text that they can use within their necessary functions (Irvine, 2024). Not all cryptography is made equal however. In fact, the more varying cryptographic methods there are, the more secure data becomes. To help with this, public key infrastructures are created to be used in a wide variety of ways. The Windows Active Directory uses this public key infrastructure to help with cybersecurity specialists creating their own key methods (Microsoft, 2023). Although Active Directory uses a system to give administrators power to manage control levels within the services that Active Directory is utilizing in the organization, key security can be an issue. Should a private key come into the public eye, all information that the key was used to encrypt would then be extremely simple to decrypt using that private key. Due to this nature of cryptography, it is important to secure key relevant information. Active Directory also gives cybersecurity analysts a number of other features to help maintain security through information. An example of this would be Active Directory’s use of certificate protocols. With encryption, Active Directory is able to attach certificate information to help cyber security analysts identify information relating to the source of a transmission (Microsoft, 2023). This can help prove the validity of online communications when a source may be disputable. Certificate information can relate to a number of different things within the exchange. Certificate Information may relate to the user that crafted and encrypted the message, the profile information the message had been handed through, Temporal metadata relating to the message in its current and past states, an authentication of anti-tamper information to ensure that the message that is being reviewed is indeed the original message in its present state relating to the first encryption used. With all of these tools, Active Directory can serve as a wonderful template for cyber security analysts to utilize in order to create their own key methods. Active directory gives a number of control schemes in order to allow qualified personnel and system administrators to personalize their encryption methods to better bolster the security of the organization, and the communications therewithin. Cryptography in general can provide a layer of security that would not be possible without the framework provided over the years to secure data (The Trustees of Indiana University, 2023). This security is further bolstered with certificate information to verify the authenticity of a transmission, and the origin of communication. With all this in mind, many tools exist within Active Directory and without in order to provide a safer and more secure data exchange no matter the party involved.

**Part 2**

**Give an example of a protocol that uses both public key and private key cryptography and explain how and why it does so.**

Cryptography can be a powerful tool to not just cybersecurity analysts, but the online population as a whole. Whether a user knows it or not, many websites visited to day utilize encryption throughout the time line of them visiting major sites. One protocol to use public and private keys during the lifetime of the network exchange would be HTTPS with Transport Layer Security (The University of Washington, 2021). During this exchange, a client and a server communicate with one another. Throughout the lifetime of this exchange, the server generates a private key, and gives the client access to a public key. These keys are used to follow and agreed upon encryption method throughout the website’s runtime. For example, without encryption any information entered on a website such as Amazon.com would be stored in plain text for any interceptor to read and utilize to malicious extent. With this setup in transport layer security in exchange is able to be made such that the client that is requesting to purchase items off of this website will encrypt secure data before sending it to the server so that if it is intercepted on the way to the server the data will be illegible to the interceptor. The data can then be decrypted using the aforementioned key setup by the server in order to get actionable information during the network exchange.

**How are the public key and private key of an asymmetrical key set related? What about this relationship makes it a “one-way” process?**

Asymmetric encryption the focus is on managing security concerns and risks associated with symmetric encryption. Utilizing an asymmetric encryption format, two clients are able to generate their own private and public keys (Chemeketa Computer Science, n.d.). For example, in client 1 a private key can be used to decrypt data while their public key can be used to encrypt it. The same is such for a second client in this exchange. The two clients would then exchange public keys, and data that needs to be utilized within the encryption process. At this time each client would have the public key of the other client. When an encryption message is sent, the public key of the sender is then used to decrypt the data. This method is a secure because public key does not have any identifying information towards the sender or receiver’s key. Because of this, losing access to one’s public key or having such information appear in a public forum does not compromise the integrity of the message, or the private key associated with it. Because of this relationship, it is also a one-way process. A single private key is not able to both encrypt and decrypt data. Same is so for public keys. Additionally, one user’s public key does not function identically to another user’s public key. For example, in order to decrypt data, the receiver is required to have a specific public key, and not just simply any public key.

# **References**

Chemeketa Computer Science. (n.d.). *Public Key Cryptography*. Retrieved from CS160 Reader: https://computerscience.chemeketa.edu/cs160Reader/NineAlgorithms/Authentication/PublicKeyCrypto.html

Irvine, T. U. (2024). *Protect Data with Encryption*. Retrieved from UCI Office of Information Technology: https://www.security.uci.edu/how-to/encryption/

Microsoft. (2023, August 10). *PKI design considerations using Active Directory Certificate Services*. Retrieved from Microsoft Learning Center: https://learn.microsoft.com/en-us/windows-server/identity/ad-cs/pki-design-considerations

The Trustees of Indiana University. (2023, June 12). *About data encryption*. Retrieved from University Information Tehcnology Services: https://kb.iu.edu/d/bgpo

The University of Washington. (2021, January 25). *Transport Layer Security*. Retrieved from ciso.uw.edu: https://ciso.uw.edu/2021/01/25/transport-layer-security/