Cryptography and C-I-A triad in Cyberwar

Truc L. Huynh, Computer Science

Purdue University Fort Wayne

**Cryptography and C-I-A triad in Cyberwar**

1. **The goal of Cryptography :**

Cryptography in cyberwarfare often involves encryption, which is a process that encodes information in a way that prevents unauthorized parties from reading the data. The cryptographic concepts rely on four major concepts: confidentiality, data integrity, authentication, and nonrepudiation.

1. **Explain four major concepts of the C-I-A triad:**

Confidentiality is the ability to ensure that data are not exposed to those who should not see them. Thus, a cryptography system that cannot be broken in a reasonable time frame can ensure confidentiality.

Data integrity is the ability to ensure that data has not been modified by its author (addition, removal, or modifying the data meaning…). Popular methods of data integrity are measuring digits or checksum the message (by use of algorithms) to compare their original and received version.

Authentication is the ability to verify the identity of a sender or receiver.

Nonrepudiation requires that it be possible to prove that the sender sends the file or message which means the sender cannot claim that someone falsely sends the message posing as them.

References

Chapple, M., & Seidl, D. (2023). Chapter 10: Cryptography and Cyberwar In *Cyberwarfare: Information Operations in a Connected World* (Second, pp. 103–124). essay, Jones & Bartlett Learning. (1)

Wikipedia (n.d.) Edward Snowden. Retrieved from <https://en.wikipedia.org/wiki/Edward_Snowden> (2)