Classwork 6

The ABCs of Cryptography

Securing the Cloud - As you watch the video consider the following questions (5.1.1 and 5.1.4):

1. What kind of information does encryption keep safe?

* Based on my understanding and analysis, encryption keeps sensitive information safe, such as personal data, financial details, passwords, and private communications. It protects data by converting it into unreadable code, ensuring that only authorized parties can access the original information.

1. Why is it important for people like Vinod to research different encryption methods?

* Based on what I have learned in the video, it is crucial for researchers like Vinod to explore different encryption methods because cybersecurity threats are constantly evolving. Developing more advanced encryption techniques ensures that sensitive data can remain secure even as hackers find new ways to breach systems.

1. What is homomorphic encryption?

* Based on my understanding and analysis, homomorphic encryption is a type of encryption that allows computations to be performed on encrypted data without needing to decrypt it. This ensures that sensitive information remains secure while still enabling data processing and analysis in the cloud.

Part 1: History of Cryptography

How Enigma Worked - As you watch the video, consider the following questions (5.2.3 and 5.2.4):

1. What was the role of the rotors in the Enigma machine?

* Based on what I learned in the video, the rotors in the Enigma machine played a crucial role in scrambling the letters of the message being encrypted. Each rotor changed the encryption key with every keystroke, creating complex and ever-changing cipher texts, making it extremely difficult to break the code.

1. What was one specific feature that, other than the rotors, made the Enigma so difficult to crack?

* Based on my understanding, another challenging feature of the Enigma machine was the plugboard, which added an additional layer of complexity by further scrambling letters before they passed through the rotors. This exponentially increased the number of possible configurations, making decryption even harder without knowing the specific settings.

Part 2: Unknown Languages - As you watch the video, consider the following questions (5.2.5 and 5.2.6)

1. How were the Ronogorongo texts different from most other written forms of language?

* Based on what I learned from the video, Ronogorongo texts were unique because they used a pictorial or glyph-based script, which makes them vastly different from phonetic writing systems. The structure and meaning behind these glyphs remain largely a mystery, adding to their complexity.

1. What advantages did the Navajo Code Talkers have over other means of cryptography?

* Based on my understanding, the Navajo Code Talkers had a significant advantage in cryptography during World War II because they used their native language, which was unwritten and unfamiliar to most people outside the Navajo community. This made it nearly impossible for enemy forces to decode their messages, giving the U.S. military a secure and efficient means of communication.

1. What makes the Ronogorongo texts nearly indecipherable?

* Based on what I have learned, the Ronogorongo texts are nearly indecipherable because there is no known bilingual text or key to decode the glyphs. Furthermore, the language used in the texts has no surviving speakers, making it difficult for modern linguists to analyze or interpret the script effectively.