Objective: These clues are designed to guide the students toward identifying the type of ransomware used in the simulation, encouraging research, analysis, and collaborative problem-solving.

Clue Packet for Teams

Clue 1: Ransom Note Characteristics

- The ransom note uses a specific font and color scheme (e.g., red text on a black background).
- It references a historical figure known for cryptography.
- The note includes a countdown timer.

Clue 2: File Extension Changes

- Affected files have had their extensions changed to an unusual suffix (e.g., ".cybersiege").
- Attempts to open these files lead to error messages.

Clue 3: Email Trail

- An email found in the inbox of a recently hired staff member contains a suspicious attachment. The email was disguised as a routine software update request.

Clue 4: Network Behavior

- The IT department noticed an unusual spike in outbound traffic from the school's servers around the time the attack was first detected.
- Several unknown IP addresses were repeatedly accessing the network.

Clue 5: Social Media Message

- A message on an obscure online forum, known for cybercriminal activities, mentions a new ransomware variant named after a famous war strategist.

Clue 6: Encryption Method

- The encryption seems to be highly sophisticated, with no known decryption tools available publicly.
- The ransom note claims that the data has been encrypted with military-grade encryption algorithms.

Clue 7: Bitcoin Wallet Activity

- The Bitcoin wallet address provided for the ransom payment has been linked to previous cyber incidents in different parts of the world.