STUDENT ACTIVITY 2.5_B: ENCRYPTION

MTA Course: 98-367 Security Fundamentals
Topic: Encryption (Part 2)
File name: SecurityFund_SA_2.5_B

Lesson Objective

2.5_B: Encryption Algorithms: Understand core security principles. *This objective may include, but is not limited to:* VPN, public key and private key, encryption algorithms, certificate properties, certificate services, PKI/certificate services infrastructure, token devices.

Resources, software, and additional files needed for this lesson

- Internet Access

Directions to the student

Research and answer the following questions.

Background: Encryption is one of several defenses-in-depth that are available to the administrator who wants to secure a server.

Encryption algorithms define data transformations that cannot be easily reversed by unauthorized users.

Questions

1. No single algorithm is ideal for all situations. Define "Basic," "Strong," and "Strongest" encryption.
2. Define "long keys."
3. Define "asymmetric encryption."
4. Define "block ciphers with long keys."
5. Why are long, complex passwords stronger than short passwords?