# STUDENT ACTIVITY 2.5_B_KEY: ENCRYPTION

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

## 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.

   **Answers:**
   Basic: For dial-up and PPTP-based VPN connections, Microsoft® Point-to-Point Encryption (MPPE) is used with a 40-bit key. For L2TP/IPSec VPN connections, 56-bit Data Encryption Standard (DES) encryption is used.
   Strong: For dial-up and PPTP VPN connections, MPPE is used with a 56-bit key.

For L2TP/IPSec VPN connections, 56-bit DES encryption is used.
Strongest: For dial-up and PPTP VPN connections, MPPE is used with a 128-bit key. For L2TP/IPSec VPN connections, triple DES (3DES) encryption is used.

**2.** Define “long keys.”

**Answer:** When we talk about the *key length* of an RSA key, we are referring to the length of the modulus, in bits. The minimum recommended key length for a secure RSA transmission is currently 1024 bits. A key length of 512 bits is now no longer considered secure, although cracking it is still not a trivial task.

**3.** Define “asymmetric encryption.”

**Answer:** There are two related keys—a key pair. A public key is made freely available to anyone who might want to send you a message. A second, private key is kept secret, so that only you know it.
Any message (text, binary files, or documents) that is encrypted by using the public key can be decrypted only by using the matching private key. Any message that is encrypted by using the private key can be decrypted only by using the matching public key.
This means that you do not have to worry about passing public keys over the Internet (the keys are supposed to be public). A problem with asymmetric encryption, however, is that it is slower than symmetric encryption. It requires far more processing power to both encrypt and decrypt the content of the message.

**4.** Define “block ciphers with long keys.”

**Answer:** DES, RC2, 3DES, Rijndael (or AES) are all block ciphers meaning that they encrypt data in blocks. DES, RC2, and 3DES have a block size of 8 bytes. AES has a block size of 16 bytes; the key size of AES can be 16 bytes, 24 bytes, or 32 bytes.

**5.** Why are long, complex passwords stronger than short passwords?

**Answer:** Each character that you add to your password increases the protection that it provides many times over. Your passwords should be 8 or more characters in length; 14 characters or longer is ideal.
Many systems also support use of the space bar in passwords, so you can create a phrase made of many words (a "pass phrase"). A pass phrase is often easier to remember than a simple password, as well as longer and harder to guess.