Security Filtering—Encryption and Remote Access

by Sophia

WHAT'S COVERED

In this lesson, you will learn about encryption, which is the process of obscuring information to make it unreadable without special knowledge, key files, or passwords.

Specifically, this lesson will cover the following:

1. Encryption

At times, sending out corporate financial and other types of sensitive data over the internet is the most convenient way to share such information. This is why being able to hide or encode that data with encryption technologies is so vital for shielding it from a company's competitors, identity thieves, or any other type of attacker. Without **encryption**, our sensitive files and information may not remain confidential as the data cross the internet.

KEY CONCEPT

Encryption works by running the data through a special encryption formula called a **key** that the designated sending and receiving devices both know. A key in cryptography is a piece of information, usually a string of numbers or letters that are stored in a file, which, when processed through a cryptographic algorithm, can

encode or decode cryptographic data. When encrypted data arrive at their specified destinations, the receiving devices uses that key to decode the data back into their original forms.

Encrypting passwords being sent from a workstation to a server when logging in is a basic need for internal networks, and most of today's network operating systems do it automatically. But legacy protocols like File Transfer Protocol (FTP) and Telnet do not have the ability to encrypt passwords. Most email systems also give users the option to encrypt email messages, and email systems that do not come with encryption abilities of their own often use third-party software packages like Pretty Good Privacy (PGP). And you already know how critical encryption is for data transmission over VPNs. Encryption capability is clearly very important for e-commerce transactions, online banking, and investing.

HINT

An encryption key is essentially a random string of characters that is used in conjunction with the encryption algorithm. The algorithm is the same for all transactions, but the key is unique to each transaction. Encryption keys come in two flavors: public and private.

TERMS TO KNOW

Encryption

The process of obscuring information to make it unreadable without special knowledge, key files, or passwords.

Key

A string of numbers or letters that are stored in a file, which, when processed through a cryptographic algorithm, can encode or decode cryptographic data.

1a. Symmetric Encryption Keys

When using **symmetric-key encryption**, both the sender and receiver have the same key and use it to encrypt and decrypt all messages. The downside of this technique is that it becomes hard to maintain the security of the key. In contrast, when the keys at each end are different, it is called **asymmetric-key encryption**. The following sections describe some symmetric-key standards and then compare them to asymmetric-key encryption.

TERMS TO KNOW

Symmetric-Key Encryption

Both the sender and receiver have the same key and use it to encrypt and decrypt all messages.

Asymmetric-Key Encryption

The sender and receiver each have their own pair of keys—one called the public key and one the private key.

1b. Data Encryption Standard (DES)

The **Data Encryption Standard (DES)** is a symmetric-key algorithm that was made a standard back in 1977 by the U.S. government. DES uses lookup and table functions, and it actually works much faster than more complex systems. It uses 56-bit keys. RSA Data Systems once issued a challenge to see if anyone could break the key.

DID YOU KNOW

A group of internet users worked together to attempt the task, with each member dealing with a portion of the 72 quadrillion possible combinations. They succeeded and cracked the key in June 1997, after searching only 18 quadrillion keys.

Back then, DES was a great security standard, but the 56-bit key length has proved to be too short.

TERM TO KNOW

Data Encryption Standard (DES)

A symmetric-key algorithm for the encryption of digital data.

1c. Triple Data Encryption Standard (3DES)

The **Triple Data Encryption Standard (3DES)**, also a symmetric-key algorithm, was originally developed in the late 1970s, and it became the recommended method of implementing DES encryption in 1999. As its name implies, 3DES is essentially three DES encryption methods combined into one.

3DES encrypts three times, and it allows us to use one, two, or three separate keys. Clearly, going with only one key is the least secure, and opting to use all three keys gives the highest level of security. Three-key 3DES has a key length of 168 bits (56 times 3).

KEY CONCEPT

One problem with 3DES is that it is slow. The National Institute of Standards and Technology (NIST) believes that 3DES will be an effective encryption standard only until sometime around 2030.

Even now, it is being phased out in favor of faster methods like AES.

TERM TO KNOW

Triple Data Encryption Standard (3DES)

A symmetric-key block cipher that applies the DES cipher algorithm three times to each data block.

1d. Advanced Encryption Standard (AES)

The **Advanced Encryption Standard (AES)** has been the official symmetric-key encryption standard in the United States since 2002. It specifies key lengths of 128, 192, and 256 bits.

KEY CONCEPT

The U.S. government has determined that 128-bit security is adequate for things like secure transactions and all materials deemed secret, but all top secret information must be encoded using 192- or 256-bit keys.

IN CONTEXT

The AES has proven amazingly difficult to crack. Those who try use a popular method involving something known as a *side channel attack*. This means that instead of going after the cipher directly,

they attempt to gather the information they want from the physical implementation of a security system. Hackers attempt to use power consumption, electromagnetic leaks, or timing information (like the number of processor cycles taken to complete the encryption process) to give them critical clues about how to break the AES system. Although it is true that attacks like these are possible to pull off, they are not really practical to clinch over the internet.

TERM TO KNOW

Advanced Encryption Standard (AES)

A symmetric-key specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001.

1e. Public-Key Encryption

Public-key encryption uses the **Diffie-Hellman algorithm**, which employs a public key and a private key to encrypt and decrypt data. This is called asymmetric encryption. It works like this: The sending machine's public key is used to encrypt a message that is decrypted by the receiving machine with its private key. It is a one-way communication, but if the receiver wants to send a return message, it does so via the same process. If the original sender does not have a public key, the message can still be sent with a digital certificate that is often called a digital ID, which verifies the sender of the message.

The diagram below shows public-key-encrypted communication between User X and User Y.

TERM TO KNOW

Diffie-Hellman Algorithm

A public-key method of securely exchanging cryptographic keys over a public channel.

1f. RSA Data Security

RSA encryption is a public-key algorithm named after the three scientists (Rivest, Shamir, and Adleman) from MIT who created it. They formed a commercial company in 1977 to develop asymmetric keys and nailed several U.S. patents. Their encryption software is used today in electronic commerce protocols.

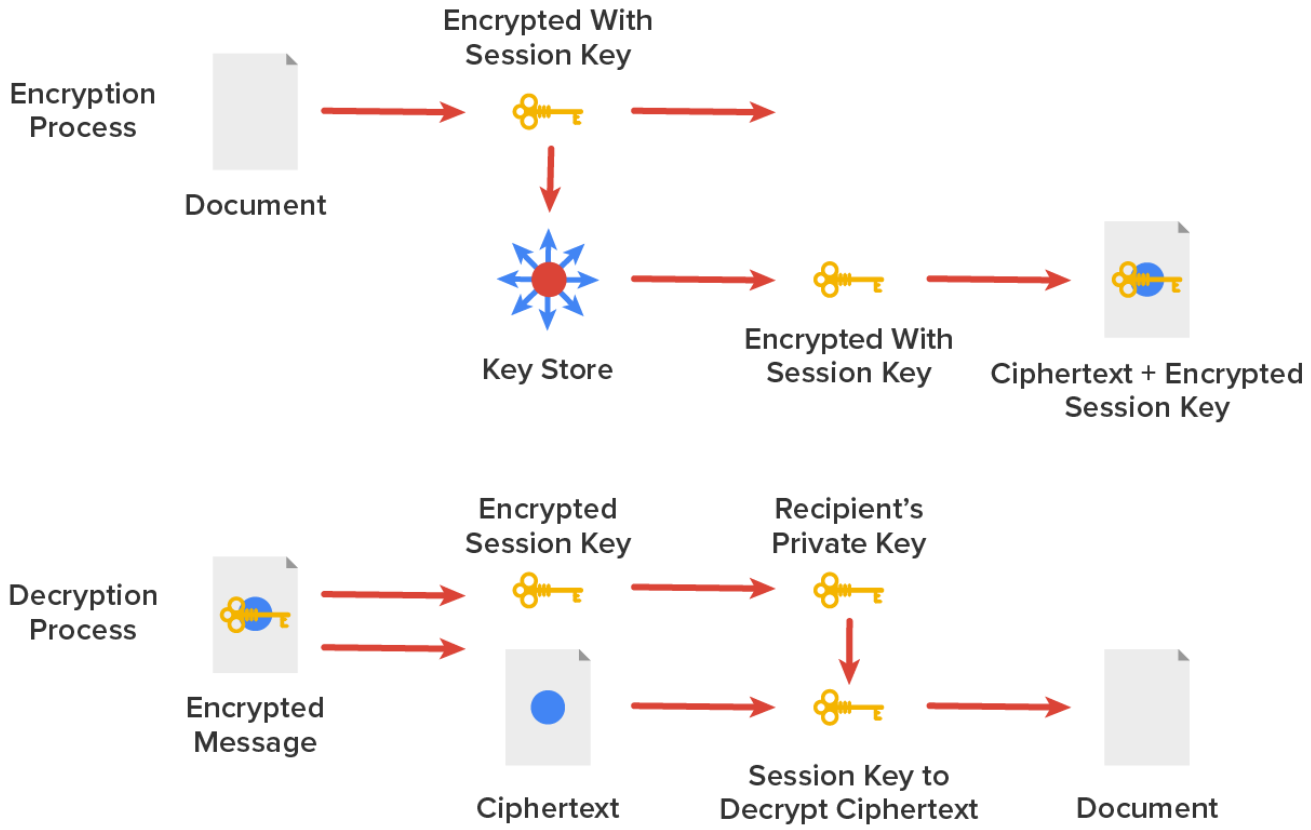
TERM TO KNOW

RSA Encryption

A public-key cryptosystem that is widely used for secure data transmission.

1g. Pretty Good Privacy (PGP)

Pretty Good Privacy (PGP) was developed in the early 1990s by Phil Zimmerman (also from MIT), who wrote most of the code for this freely available version of public-key encryption designed to encrypt data for email transmission. Zimmerman basically compared email to postcards, because anyone can read email messages traversing the internet just as they can postcards traveling through the postal service. By contrast, he compared an encrypted message to a letter mailed inside an envelope. The diagram below shows the PGP encryption system.



In the diagram above, the document is encrypted with a session key, which is then encrypted with the public key of the recipient. Then the ciphertext and the encrypted session key are sent to the recipient. Since the recipient is the only person with the matching private key, only they can decrypt the session key and then use it to decrypt the document.

IN CONTEXT

Zimmerman distributed the software for personal use only, and as the name implies, it is really pretty good security. RSA Data Security and the U.S. federal government both had a problem with Zimmerman's product—the RSA complained about patent infringement, and the government actually decided to prosecute Zimmerman for exporting munitions-grade software. The government eventually dropped the charges, and now a licensing fee is paid to RSA, so today, PGP and other public-key-related products are readily available.

TERM TO KNOW

Pretty Good Privacy (PGP)
An encryption program that provides cryptographic privacy and authentication for data communication.

SUMMARY

In this lesson, you learned about **encryption**, including **symmetric and asymmetric encryption keys**. This included the **Data Encryption Standard (DES)**, **Triple Data Encryption Standard (3DES)**, **Advanced Encryption Standard (AES)**, **Public-Key Encryption**, **RSA Data Security**, and **Pretty Good Privacy (PGP)**.

Source: This content and supplemental material has been adapted from CompTIA Network+ Study Guide: Exam N10-007, 4th Edition. Source Lammle: CompTIA Network+ Study Guide: Exam N10-007, 4th Edition - Instructor Companion Site (wiley.com)

TERMS TO KNOW

Advanced Encryption Standard (AES)
A symmetric-key specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001.

Asymmetric Key Encryption
The sender and receiver each have their own pair of keys—one called the public key and one the private key.

Data Encryption Standard (DES)
A symmetric-key algorithm for the encryption of digital data.

Diffie-Hellman Algorithm

A public-key method of securely exchanging cryptographic keys over a public channel.

Encryption

The process of obscuring information to make it unreadable without special knowledge, key files, or passwords.

Key

A string of numbers or letters that are stored in a file, which, when processed through a cryptographic algorithm, can encode or decode cryptographic data.

Pretty Good Privacy (PGP)

An encryption program that provides cryptographic privacy and authentication for data communication.

RSA Encryption

A public-key cryptosystem that is widely used for secure data transmission.

Symmetric-Key Encryption

Both the sender and receiver have the same key and use it to encrypt and decrypt all messages.

Triple Data Encryption Standard (3DES)

A symmetric-key block cipher that applies the DES cipher algorithm three times to each data block.