7.1.2 Cryptography Facts

The goal of all IT security specialists is to keep data safe. Hackers find ways to circumvent firewalls, IPS devices, and other security protocol put in place. Cryptography is one additional layer of defense that can be used to protect data.

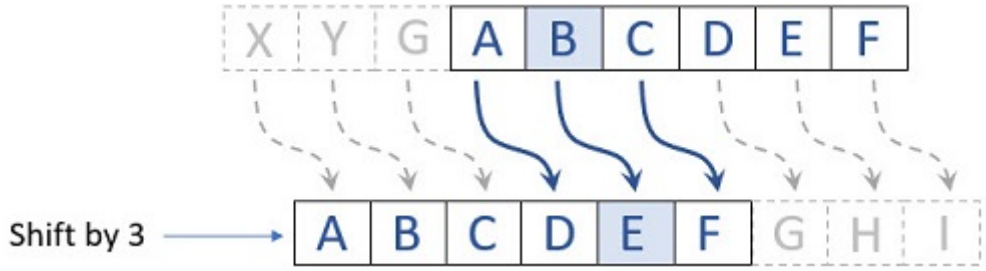
This lesson covers the following topics:

- Cryptography overview
- Cryptography concepts
- Cryptography methods

Cryptography Overview

Cryptography is defined as the process of writing or solving messages using a secret code. A form of cryptography called encryption has been used throughout the ages, mainly to keep messages out of the hands of enemies. Encryption is the process of converting normal readable text into something that is unintelligible called ciphertext. A cipher is the method, or algorithm, used to encrypt or convert the data.

One of the more popular forms of encryption is the Caesar cipher. This encryption method works be shifting each letter in the alphabet a certain number of spaces to the right or left. In the example below, the cipher is shifting to the right by three letters. A becomes D, B becomes E, C becomes F, and so forth.



To decrypt the message, the reader must know how many spaces to shift the letters. For example, to encrypt the word TESTOUT using the Caesar Cipher with a shift of 3 to the right, TESTOUT would become WHVWRXW.

Below is the complete Caesar cipher using a shift of three letters to the right (you can see below which letters are used when they are shifted 3 spaces):

This is a very simple example of cryptography and is easily decrypted. With today's computing power, encryption methods used are much more complicated and powerful.

Cryptography Concepts

There are three main concepts to understand when dealing with today's encryption methods: encryption keys, hashing, and digital signatures.

Cryptography Concept	Description
Encryption keys	Encryption keys are used to encrypt and decrypt data. The key is a string of bits that is randomly generated using a specific cipher, such as Advanced Encryption Standard (AES). There are two types of encryption methods used with keys: symmetric and asymmetric. ▪ Symmetric encryption uses the same key to encrypt and decrypt data. ▪ Asymmetric encryption uses one key to encrypt the data and a different key to decrypt the data. These keys are known as a public key and private key.
Hashing	Hashing is the process of converting one value into another using a mathematical algorithm like MD5 or SHA. This fixed length of data is called the hash. ▪ Hashing is used on data that does not need to be decrypted, such as a password. ▪ When a piece of data is run through a hashing algorithm, it always generates the same hash. If even one letter in a file has been altered, the resulting hash would be different. Because of this, hashing can be used to verify that data has not been altered during transmission. ▪ A hash cannot be decrypted. However, when using hashing for passwords, many online sites have collected massive databases containing a hash for tens of millions (or more) of possible passwords. Once a hash has been captured, it can be compared with the hashes found in the database, quickly resulting in the password used to create the hash.
Salt	Salt, or salting the hash, means that a random number of characters are added to the password before the hash is created. For example, if the password to be hashed was p@ssw0rd, a salt, such as E1343135E119C253, may be added. Therefore, the string to be hashed would be p@ssw0rdE1343135E119C253. Since the salt is randomly generated each time, even if the same password is used and is of varying lengths, it's virtually impossible to create a database containing all the possible salted passwords.
Digital signatures	By combining a user's private encryption key and a hash of the data, a user can create a digital signature. A digital signature verifies that the data is legitimate and provides non-repudiation. This means that the sender cannot deny having sent the file.

Cryptography Methods

There are many different cryptography methods used today. One important thing to keep in mind is that all cryptography uses advanced math concepts to generate encryption keys and hashes.

Cryptography Method	Description
Elliptic Curve Cryptography (ECC)	Elliptic Curve Cryptography is one of the newer methods being implemented. ECC is able to generate smaller keys that are more secure than most other methods. Many websites today use ECC to secure connections and data transmissions.
Perfect Forward	This cryptography method is used quite often in messaging apps. Instead of the same key being used for an entire conversation or session on a website, each transmission is

Secrecy	encrypted with a different unique key.
Steganography	Steganography is the technique of hiding or concealing a file, message, image, or video within another file, message, image, or video. Special programs are often used to hide messages in media files. If a hacker intercepts the message, all they see is the media. They don't know that there is a hidden message.