7.2.2 Cryptography Uses and Limitations Facts

When properly implemented, cryptography methods can be used to support the goals of information security. This is true in all cases except availability. Encryption and decryption can slow the availability of data.

This lesson covers the following topics:

- Uses of cryptography
- Limits of cryptography

Uses of Cryptography

The following table shows how cryptography can be used to support the goals of Information Security.

Information Security Goal	Cryptography support
Confidentiality	Encrypting data or obfuscating data provides data confidentiality. Obfuscation is different than encryption, but is a form of cryptography. ▪ Encryption is the process of transforming readable data into something unreadable. This is called ciphertext. ▪ Obfuscation is the process of making something more difficult to understand without changing the data itself.
Integrity	Creating a hash of a file can be used to validate that the file has not been altered. This validates the integrity of the file.
Authenticity	Applying a digital signature proves that the file is authentic and comes from the correct person.
Non-repudiation	Applying a digital signature provides non-repudiation. This means that the sender cannot later deny having sent the file.

Limits of Cryptography

Implementing cryptography does come with some limitations. The following table covers some of these limitations.

Limitation	Description
Speed	Speed is one of the biggest limitations of encryption. The encryption process can take a long time, especially with the large file sizes in use today. For example, BitLocker encrypts 500 megabytes in approximately 1 minute. A 2TB drive would take approximately 67 hours to encrypt.
Resources	Encryption is done through advanced algorithms and mathematical operations. This requires a large amount of CPU power and resources.
Weakness in keys	Encryption keys can be a weakness depending on how they are utilized. ▪ Re-use. Re-using keys is a major concern. The more a key is re-used, the more likely it is

	▪ Reuse - Reusing keys is a major concern. The more a key is reused, the more likely it is that it will be cracked. For best security, a key should be used only one time. ▪ Key Length - Encryption keys should be no less than 256 bits. For better security, using an algorithm such as AES that also uses a 128-bit block size is ideal. ▪ Predictability - A predictable key is susceptible to a dictionary attack. Strong keys are completely random. If the number generator used is not random enough, the keys are weaker. This lack of randomness is called entropy. ▪ Longevity - The longer an encryption standard is used, the more likely it is that it will be cracked. Computer scientists are constantly working on newer, more secure methods of encryption.
Availability	Availability of data is one of the goals of Information Security. Since encryption can hinder the availability of data, it is important to measure the level of security against the availability of a resource. The more secure data is made, the more difficult (less available) it becomes for a user to access.