15.6.2 Encryption Facts

Encryption is a security technique that encodes information so that only someone with the proper key can decode it.

This lesson covers the following topics:

- Types of encryption
- Encryption standards

Types of Encryption

There are two encryption types:

Type	Description
Symmetric	Symmetric key encryption (also known as secret key encryption, pre-shared key or private key encryption) uses only one key to encrypt and decrypt data. ▪ Symmetric encryption is well suited for bulk encryption, because it is less CPU-intensive and much faster than other encryption methods. ▪ Before communications begin, both parties must exchange the shared secret key using a secure channel. This is often done manually or with some form of asymmetric key cryptography. ▪ Each pair of communicating entities requires a unique shared key. ▪ As the number of bits in the key increases, so does the strength of the encryption. However, the greater the number of bits in the key, the more CPU resources are required to perform the encryption.
Asymmetric	Asymmetric encryption (also known as public key encryption) uses two keys that are mathematically related. Both keys together form a key pair. ▪ The public key is made available to anyone; the private key is kept secret. ▪ Data encrypted with the public key can only be decrypted using the private key. Data encrypted with the public key cannot be decrypted using the same public key. ▪ The strength of an asymmetric encryption system lies in the security of its private keys. If the private key is ever compromised, a new key pair must be generated. ▪ Asymmetric encryption is slower than symmetric encryption and is CPU-intensive. Processing speeds are much slower than symmetric key encryption.

Encryption Standards

Standards for symmetric and asymmetric encryption include:

Type	Description
Symmetric	*Data Encryption Standard* (DES) is an old encryption standard created by the National Security Agency in the 1970s. DES uses weak encryption and can be easily broken.
Triple DES (3DES) is an enhanced version of DES. 3DES applies DES three times and uses a 168-bit key.	
Advanced Encryption Standard (AES) is a stronger encryption system that supports encryption key lengths up to 256 bits. AES is based on the *Rijndael cipher* developed by Joan Daemen and Vincent Rijmen.	
Blowfish is an older encryption system designed to replace DES. Blowfish uses 64-bit blocks and key lengths anywhere from 32 bits to 448 bits.	
Asymmetric	*Rivest, Shamir, and Adleman* (RSA) is based on factoring large numbers into their prime values. RSA supports key-lengths from 1,024 to 4,096 bits.
Digital Signature Algorithm (DSA) is a United States Government encryption standard often used for digital signing. DSA currently supports *Secure Hashing Algorithm-1* (SHA-1), which uses key lengths between 160 and 256 bits, or SHA-2, which uses key lengths between 256 and 1024 bits.	

Diffie-Hellman Key Exchange was developed by Whitfield Diffie and Martin Hellman. It is a *key agreement protocol* that generates symmetric keys simultaneously at sender and recipient sites over non-secure channels. The Diffie-Hellman key exchange:

- Provides for key distribution and does not provide any cryptographic services.
- Is based on calculating discreet logarithms in a finite field.
- Is used in many algorithms and standards.
- Is subject to man-in-the-middle attacks and requires strong authentication to validate the endpoints.