

Real-World Scenario 14-3: Understanding Symmetric and Asymmetric Algorithms

Scenario: You have been tasked with selecting cryptographic algorithms for internal storage and Internet-based transmissions. Select the strongest symmetric and asymmetric algorithms possible for each situation.

What algorithm should you select to encrypt an entire hard drive on a laptop?

What asymmetric algorithm should you select for the key exchange during a login to a secure website (using HTTPS)?

What symmetric algorithm should you select for the data exchange during a secure web session?

Real-World Scenario 14-3 Solution

It's a fact: there are lots of cryptographic algorithms to choose from, but the ones that are the most secure make up a pretty short list. The key here (pun intended) is to select algorithms that will secure data as best possible, while working quickly to do so. The following answers are examples. You might find other answers that better suit your needs, and of course, new algorithms are released periodically.

The most common algorithm used for whole disk encryption (such as BitLocker) is AES. AES 256-bit is preferred. This is a symmetric algorithm that uses a block cipher.

There are three excellent answers for secure key exchange over the Internet; they are all asymmetric. First is RSA 2048-bit. It is commonly used by websites, but it has a massive key length, so elliptic curve technologies are also used: the Diffie-Hellman version ECDH (or ephemeral version ECDHE) and the DSA version (ECDSA). These use less computational power because the elliptic curve method uses a shorter key length.

The best symmetric algorithm for data exchange during a secure web session is AES; however, you might also see RC4 used. In fact, some websites will offer AES connections until too many users are connected simultaneously; at that point, the additional users will receive RC4-based certificates.

Video Solution: Watch the video solution “14-3: Understanding Symmetric and Asymmetric Algorithms.”

This video was recorded in 2014. It shows SHA-1 being used by a couple of websites. Remember that SHA-1 was deprecated as of 1/1/2017 and should be replaced by a more powerful cryptographic hash.

Simulation: Complete the simulation “14-3: Understanding Symmetric and Asymmetric Algorithms.”