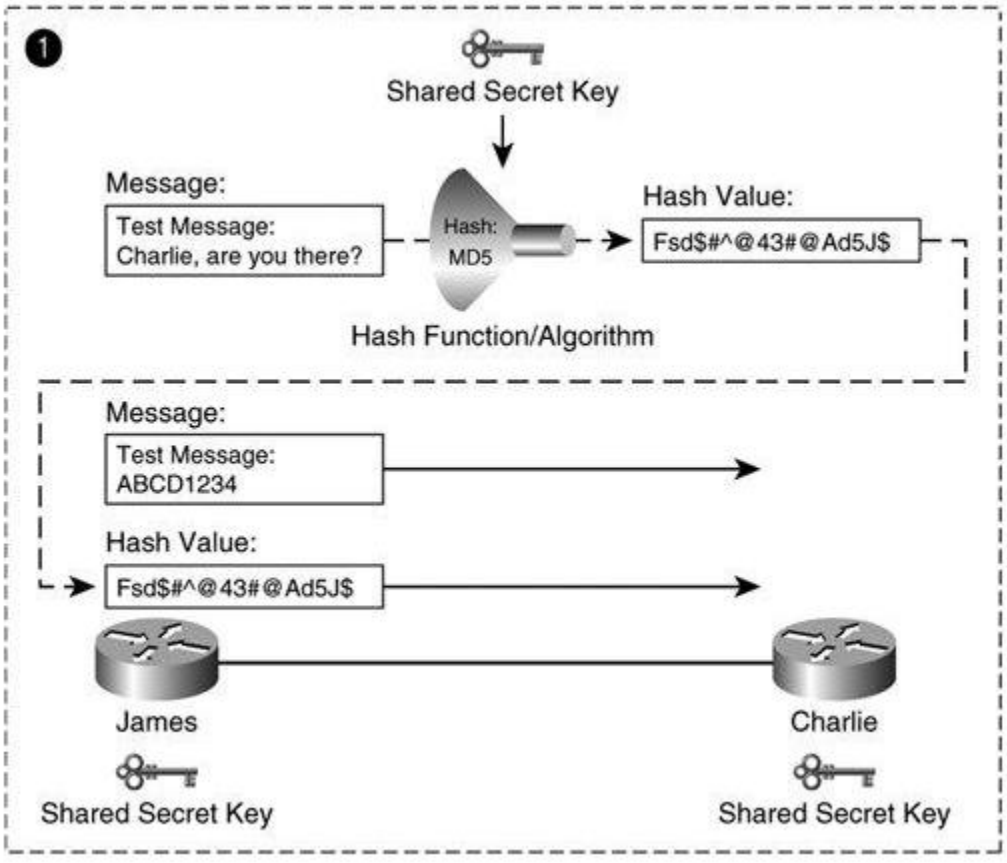
IPsec Message Authentication, Message Integrity, and Sender Nonrepudiation Mechanisms.

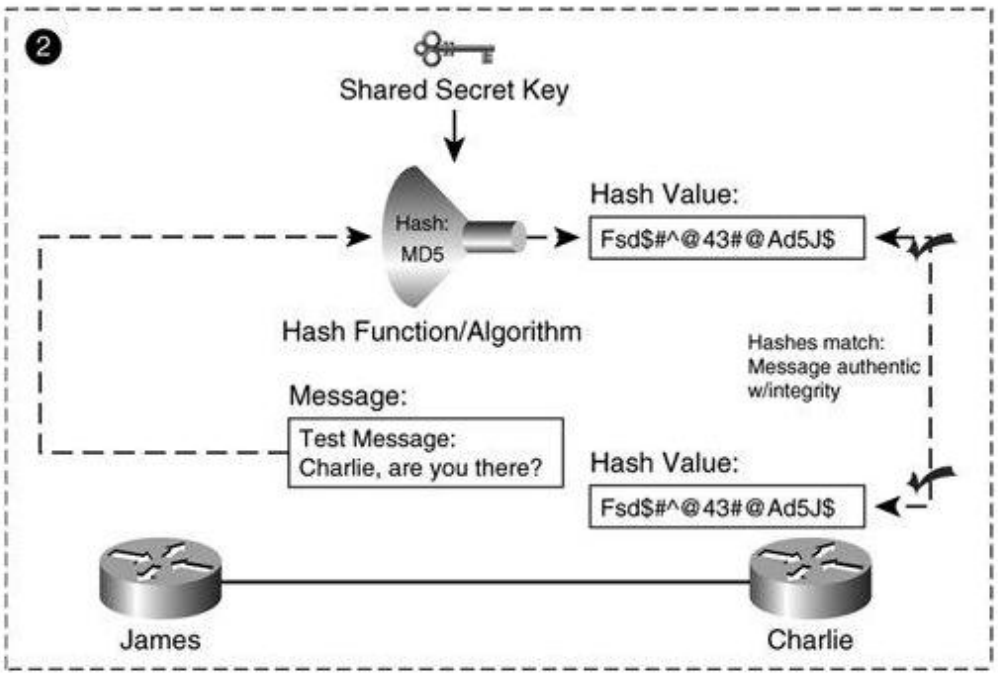
IPsec incorporates several cryptographic operations to ensure message authenticity, data integrity, and sender nonrepudiation. In this section, we will describe the mechanics of these cryptographic operations, including message hashing and message digests.

Hashing and Message Digests

Data Integrity ensures that transmitted data has not been tampered with route to its destination. Hashes can be deployed to ensure data integrity. A hash takes an input message of variable length and output fixed-length code. The fixed length code is then appended to the original message before transmission. A basic hashing function consists of an algorithm and a key that is known to both sender and receiver.

Creating and Verifying a Message Digest





Before sending his message to Charlie in Step 1, James performs a mathematical operation, or hashing function, on the original message. The output of that mathematical operation is called a hash value, or message digest, which is then appended the original message and sent to Charlie.
In Step 2, Charlie then removes the hash value from the original message and runs the same hash operation on the original message received. Charlie then compares his hash value with the one that James had sent appended to the original message. If the two hash values match, then Charlie can be assured that the message's integrity has not been compromised. That is to say that James message to Charlie has not been spoofed by a source other than James himself.

Although message digests provide data integrity, they do not provide message authenticity unless the original message is hashed with a secret key shared between the two endpoints. This operation is commonly used in routing protocol authentication and also in the creation of hashed message authentication codes (HMACs) used for bulk data encryption by a symmetric key transform defined an IPsec SAs.

In order for a hash to effectively provide data integrity, the hash operation must have the following characteristics:

- Identical input messages must consistently yield the same output.
- The input message length can very, but the length of the output of the hash operation must be of fixed length.
- The output must be random, or one way one should never be able to determine the original message by reversing the hash operation.
- It must be irreversible, or one way one should never be able determine the original message by reversing the hash operation.
- Each unique input message should yield a unique output value.

The most widely used hash algorithms are the Secure Hash Algorithm (SHA) and the Message Digest algorithm (MD5). Both MD5 and SHA process input in 512-bit blocks, but the length of their output varies MD5 outputs a 128-bit message digest, while the message digest output of SHA is 160 bits. As such, SHA is considered a stronger hash, but requires more processing power than the MD5 hash algorithm.