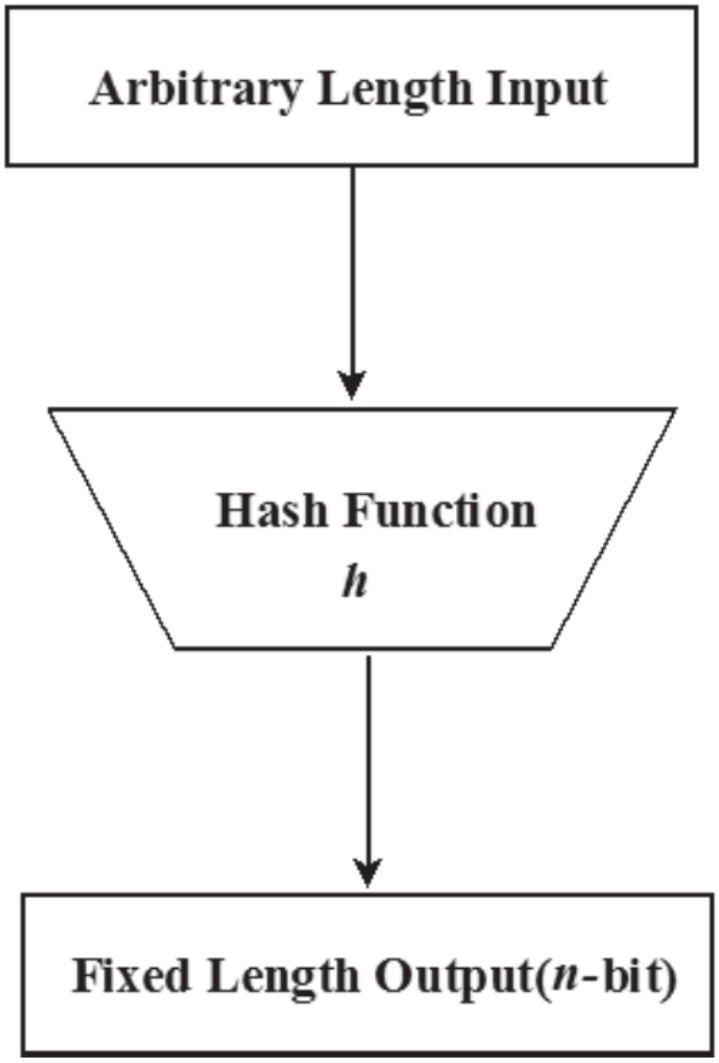
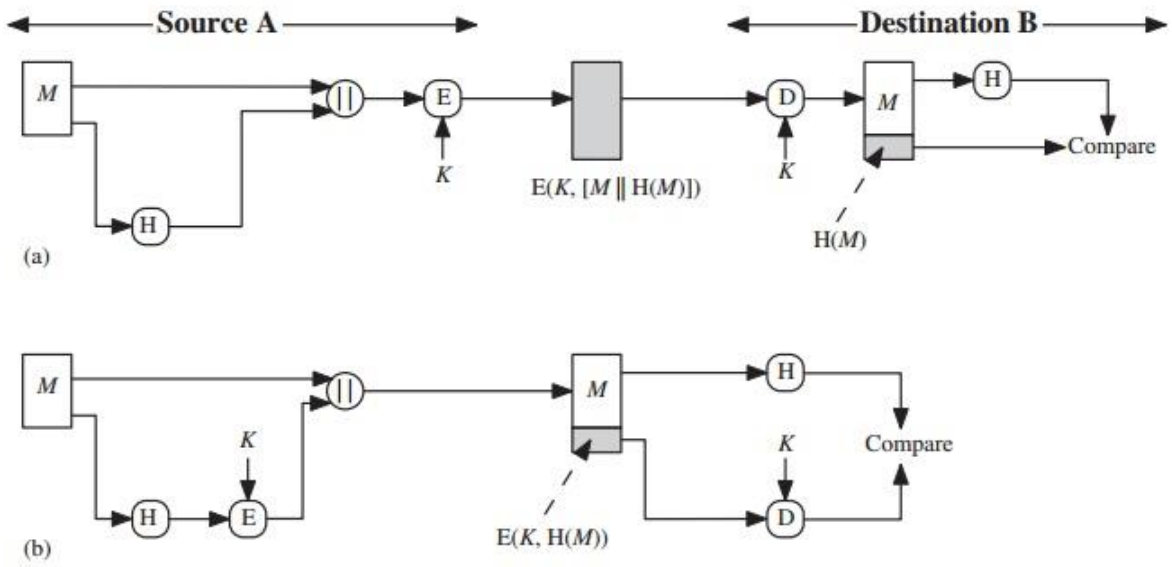
Basics of Cryptographic Hash Function

A hash function maps a variable-length message into a fixed-length hash value, or message digest. A hash function H accepts a variable-length block of data as input and produces a fixed-size hash value h = H(M). The kind of hash function needed for security applications is referred to as a cryptographic hash function.



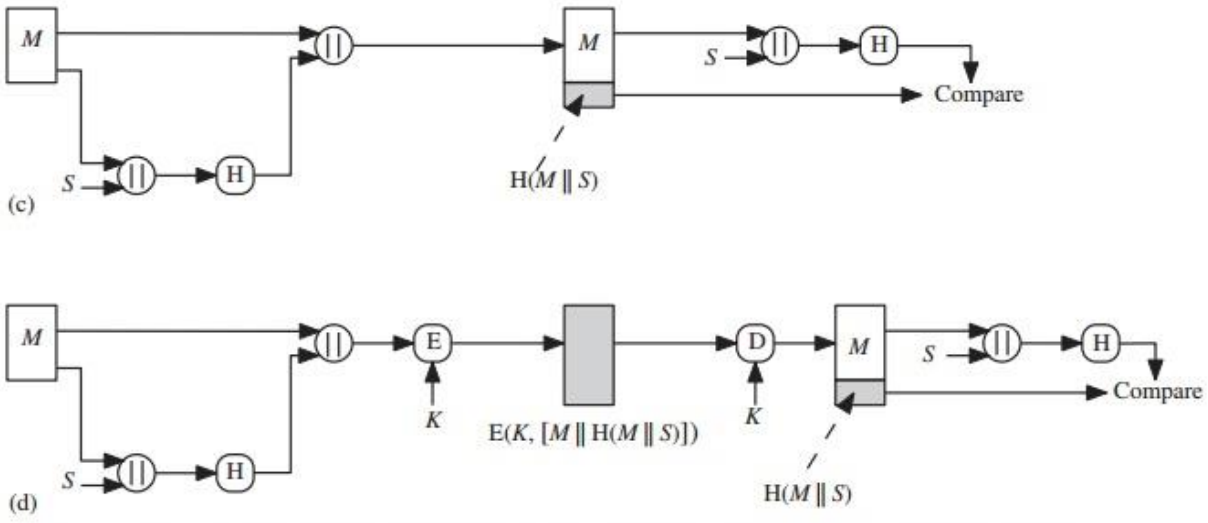
Cryptographic Hash Function and Message Authentication

Hash functions are often used to determine whether or not data has changed. Message authentication is a mechanism or service used to verify the integrity of a message. Message authentication assures that data received are exactly as sent. When a hash function is used to provide message authentication, the hash function value is often referred to as a message digest.



In the case of figure (a): The message plus concatenated hash code is encrypted using symmetric encryption. Because only A and B share the secret key, the message must have come from A and has not been altered. The hash code provides the structure or redundancy required to achieve authentication. Because encryption is applied to the entire message plus hash code, confidentiality is also provided.

In the case of figure (b): Only the hash code is encrypted, using symmetric encryption. This reduces the processing burden for those applications that do not require confidentiality.

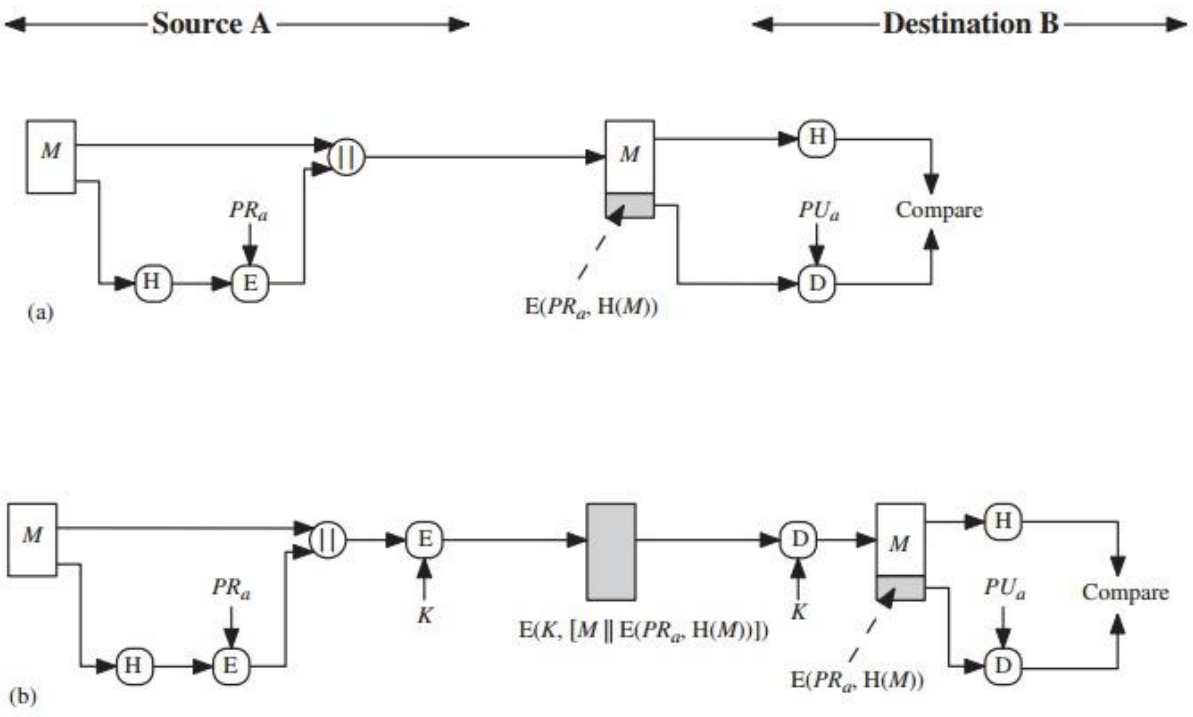


In the case of figure (c): It is possible to use a hash function but no encryption for message authentication. The technique assumes that the two communicating parties share a common secret value S. A computes the hash value over the concatenation of M and S and appends the resulting hash value to. Because B possesses the knowledge of S, it can recompute the hash value to verify. Since the secret value itself is not sent, an opponent cannot modify an intercepted message and cannot generate a false message.

In the case of figure (d): Confidentiality can be added to the approach of (c) by encrypting the entire message plus the hash code.

Cryptographic Hash Function and Digital Signature

In the case of the digital signature, the hash value of a message is encrypted with a user's private key. Anyone who knows the user's public key can verify the integrity of the message that is associated with the digital signature. In this case, an attacker who wishes to alter the message would need to know the user's private key.



In case of (a): The hash code is encrypted, with the sender's private key. It also provides a digital signature, because only the sender could have produced the encrypted hash code. In fact, this is the essence of the digital signature technique.

In case of (b): If confidentiality as well as a digital signature is desired, then the message as well as the private-key encrypted hash code can be encrypted using a symmetric secret key.