This could happen as a result of a person–in–the–middle attack. When this new message and digest arrive at the receiver, the hash test indicates that all is well and the recipient incorrectly assumes that the integrity of the message has not been compromised. In such an attack the message and digest are intercepted, the message is changed and a new digest is generated by applying the hash function to the new message.

Summarized by © lakhasly.com