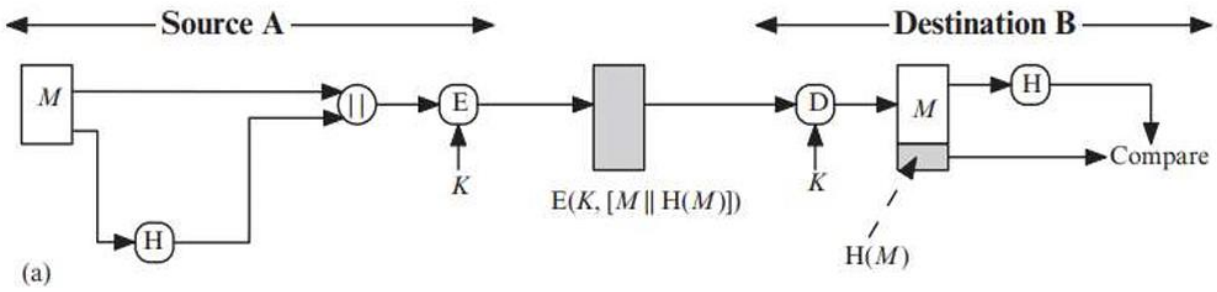

Figure (a): Hash with Symmetric Encryption

1. **Source A:**
   - The message M is processed through a hash function $H(M)$, which generates a fixed-length hash.
   - The original message M is then concatenated with its hash $H(M)$ using concatenation operator $||$.
   - The concatenated result $M||H(M)$ is encrypted with a symmetric key K, resulting in $E(K, [M||H(M)])$.
2. **Destination B:**
   - Upon receiving the encrypted message, Destination B decrypts it using the same symmetric key K, retrieving $M||H(M)$.
   - The message M is then hashed locally, and the received hash $H(M)$ is compared with the newly computed hash.
   - If both hashes match, the message is confirmed to be authentic and unaltered.

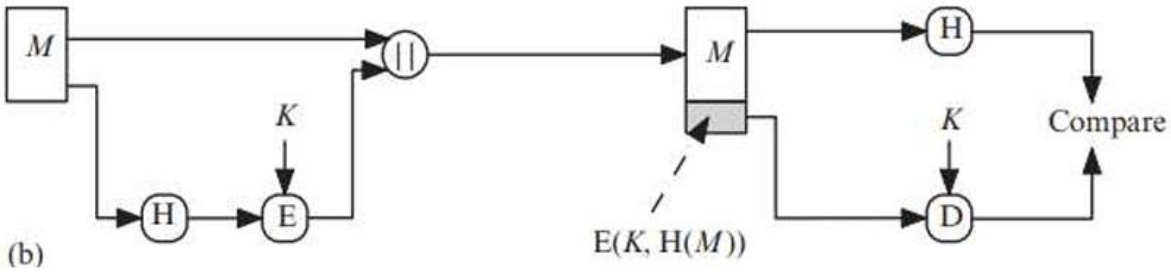

Figure (b): Symmetric Key with Hash Encryption

1. **Source A:**
   - The message M is hashed to generate $H(M)$.
   - The hash $H(M)$ itself is encrypted using the symmetric key K to get $E(K, H(M))$.
   - The original message M and the encrypted hash $E(K, H(M))$ are concatenated and sent to the destination.
2. **Destination B:**
   - Upon receiving the message M and the encrypted hash $E(K, H(M))$, Destination B decrypts the hash using K, retrieving the original hash $H(M)$.
   - Destination B then hashes the received message M and compares the locally computed hash with the decrypted hash.
   - If they match, it confirms the message's integrity and authenticity.

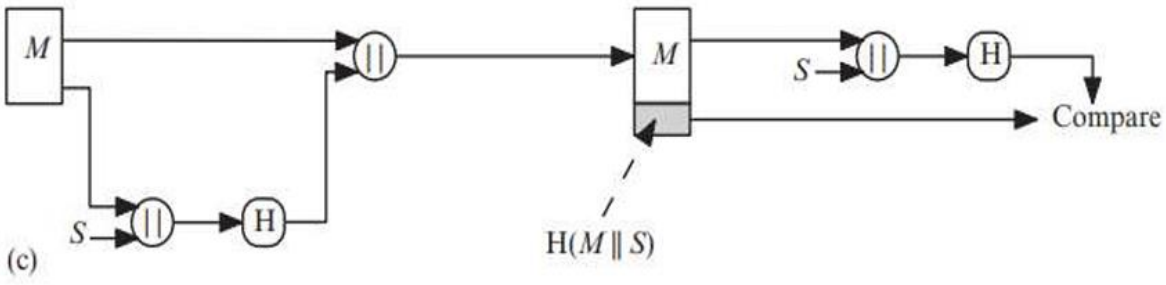

Figure (c): Message and Secret Concatenation (without Encryption)

1. **Source A:**
   - A secret S is combined with the message M using concatenation $M||S$.
   - The hash of the concatenated string $H(M||S)$ is computed and sent alongside the message M.
2. **Destination B:**
   - The destination receives both the message M and the hash $H(M||S)$.
   - Destination B locally concatenates the message with the shared secret S, computes $H(M||S)$, and compares it with the received hash.
   - If the hash matches, it verifies the message integrity.

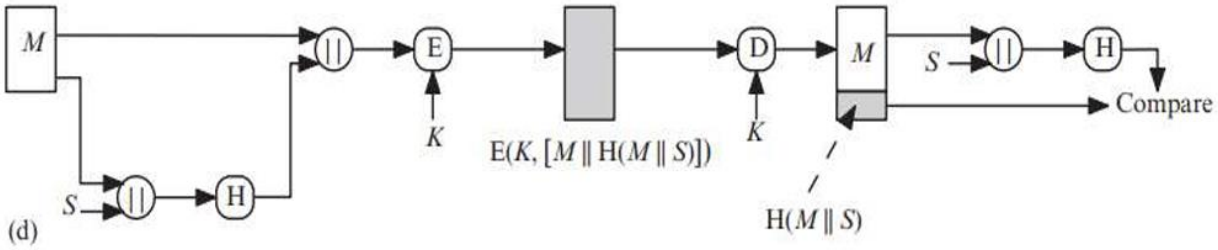

Figure (d): Secret-Based Hash with Symmetric Encryption

1. **Source A:**
   - Similar to figure (c), the message M is concatenated with a secret S.
   - The hash $H(M||S)$ is computed, and then both the message M and the hash $H(M||S)$ are concatenated.
   - This entire concatenated string is encrypted using a symmetric key K, resulting in $E(K, [M||H(M||S)])$.
2. **Destination B:**
   - Upon receiving the encrypted message, Destination B decrypts it using the symmetric key K, extracting $M||H(M||S)$.
   - It then computes the hash $H(M||S)$ based on the shared secret S and compares it to the received hash.
   - If the hashes match, it confirms that the message has not been tampered with and is authentic.