There are plethora of algorithms is vulnerable to man in the middle attack.

1. Message Authentication Codes

Encryption != integrity.

Definition short piece of information used for authentication and integrity checking a message.

Non-repudiation is a security assurance that prevents signers from denying their actions.

MACs are not resistant to non-repudiation, because minimum two sides know secret key - so anyone can make message. In contrast with digital signatures, where asymmetric keys is used.

2. HMAC

Def MAC with used hashing. resists length extension attacks, add more security by using random oracle.

3. Lamport auth

A generates "root" and $(1...n) \in N, n : H(\texttt{root})^n$ A passes to B H(root)^n. The next time A passes to B $H(\texttt{root})^{n-1}$ So either A found a collision, or A knows hash key.

4. Chinese remainder theorem

Given k coprime numbers. And system:

$$x \equiv a_1 \bmod n_1$$

$$x \equiv a_2 \bmod n_2$$

$$...$$

$$x \equiv a_k \bmod n_k$$

Then exists $x \equiv n_1 * n_2 * ... * n_k$

5. Hidden subgroup problem