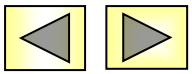
# §5.1 概述

网络系统安全要考虑两个方面。一方面，用密码保护传送的信息使其不被破译；另一方面，就是防止对手对系统进行主动攻击，如伪造，篡改信息等。

认证（**authentication**）则是防止主动攻击的重要技术，它对于开放的网络中的各种信息系统的安全性有重要作用。

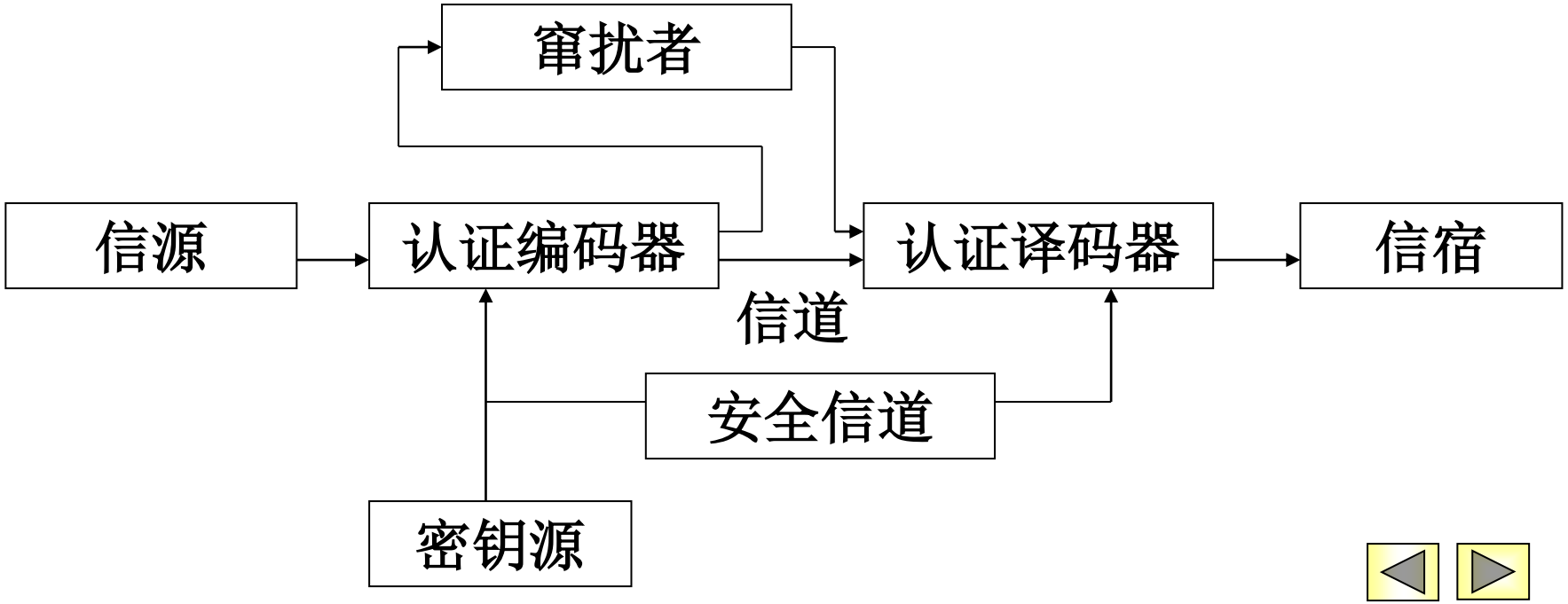
认证的主要目的：第一，验证信息的发送者是真的，而不是冒充的，此为实体认证，包括信源、信宿等的认证和识别； 第二，验证信息的完整性，此为消息认证，验证数据在传送或存储过程中未被篡改，重放或延迟等。



# §5.1 概述

保密和认证同时是信息系统安全的两个方面，但它们是两个不同属性的问题，认证不能自动地提供保密性，而保密也不能自然地提供认证功能。

一个纯认证系统的模型如下图所示：



# §5.1 概述

消息认证是一种过程，它使得通信的接收方能够验证所收到的报文（发送者和报文内容、发送时间、序列等）在传输的过程中没有被假冒、伪造和篡改，是否感染上病毒等，即保证信息的完整性和有效性。

消息认证的目的在于如何让接收报文的目的站来鉴别报文的真伪，消息认证的内容应包括：

（1）证实报文的源和宿；

（2）报文内容是否曾受到偶然的或有意的篡改；

（3）报文的序号和时间栏。

认证只在相应通信的双方之间进行，而不允许第三者进行上述认证。认证不一定是实时的。