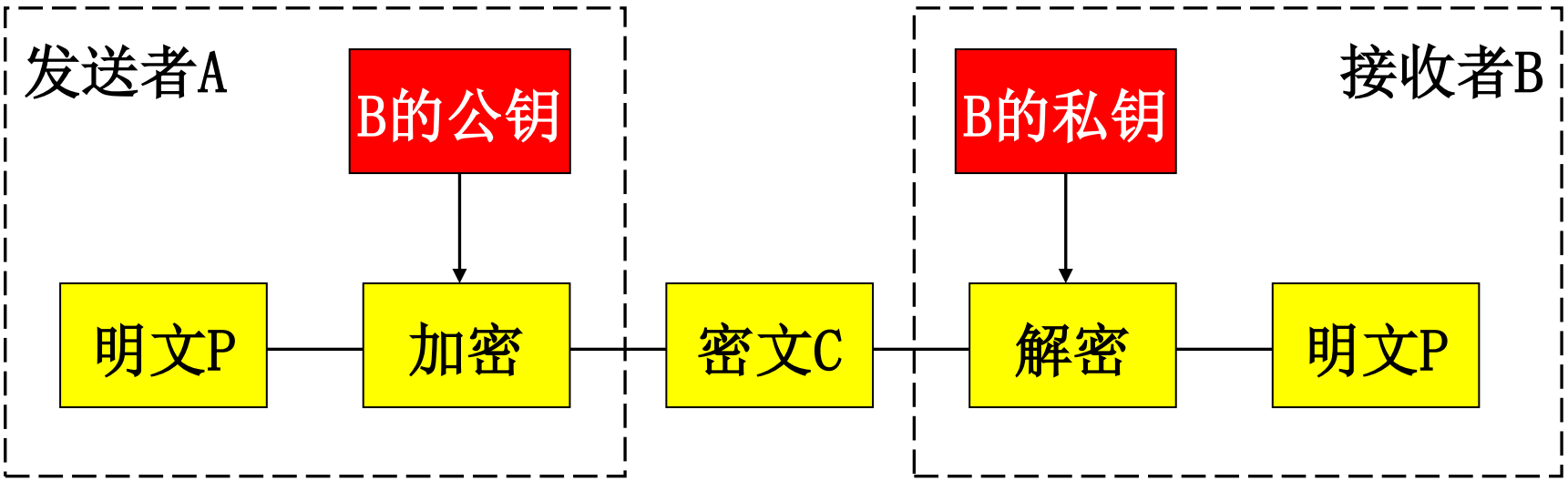
§4.1 概述

- 尽人皆知的密钥叫做公开密钥(public key)；
- 只有密钥拥有者才知道的密钥：私有密钥(private key) ；
- 这两种密钥合在一起称为密钥对；
- 公开密钥可以解决安全分配密钥问题（不需要与保密密钥通信，所传输的只有公开密钥，它不需要保密），但对保证其真实性和完整性却非常重要。
- 如果某一信息用公开密钥加密，则必须用私有密钥解密，这就是实现保密的方法。
- 如果某一信息用私有密钥加密，它必须用公开密钥解密，这就是实现验证的方法。

§4.1 概述

公开密钥密码体制算法的特点：使用一个加密算法E和一个解密算法D，它们彼此完全不同，根据已选定的E和D，即使已知E的完整描述，也不可能推导出D。

公开密钥密码体制如图



§4.1 概述

使用公开密钥加密算法进行数字签名：书信或文件是根据亲笔签名或印章来证明其真实性的。但在计算机网络中传送的文件又如何盖章呢？这就是数字签名所要解决的问题。

数字签名必须保证做到以下3点：

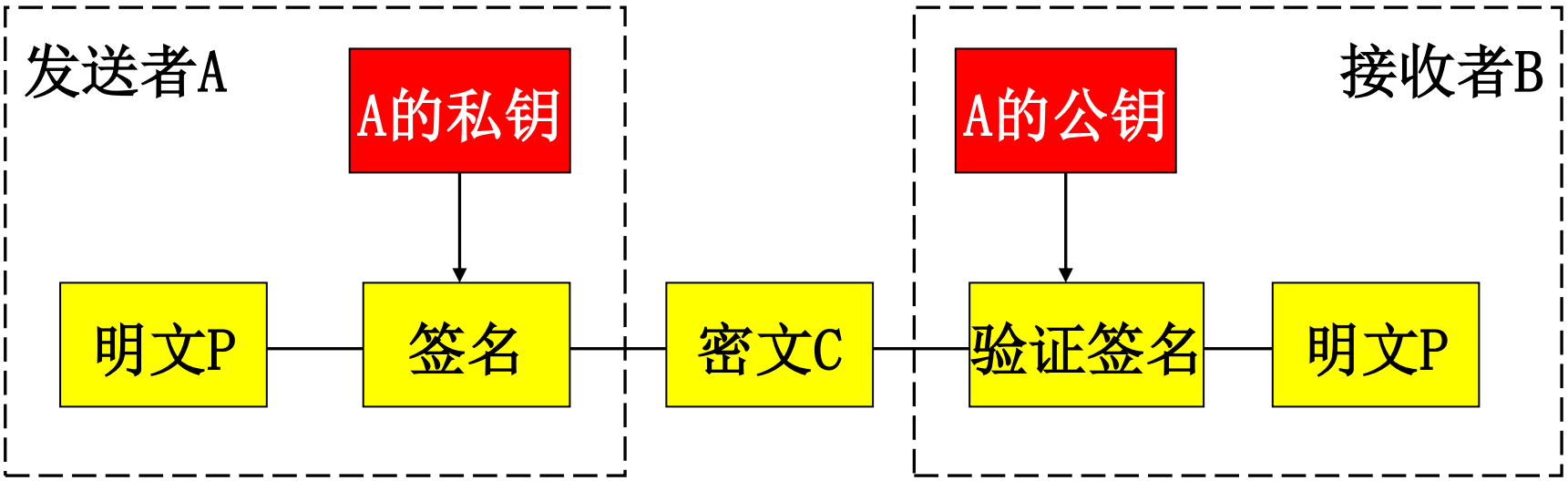
（1）接收者能够核实发送者对报文的签名；

（2）发送者事后不能抵赖对报文的签名；

（3）接收者不能伪造对报文的签名。

§4.1 概述

数字签名的实现如图



§4.2 RSA公钥密码体制

RSA是一种基于公钥密码体制的优秀加密算法，1978年由美国麻省理工学院(MIT)的研究小组成员：李维斯特(Rivest)、沙米尔(Shamir)、艾德曼(Adleman)提出的。

RSA算法是一种分组密码体制算法，它的保密强度是建立在具有大素数因子的合数，其因子分解是困难的（基于大数分解的难度）。

公钥和私钥是一对大素数的函数，从一个公钥和密文中恢复出明文的难度等价于分解两个大素数之积。

RSA得到了世界上的最广泛的应用，ISO在1992年颁布的国际标准X.509中，将RSA算法正式纳入国际标准。