HTTPS

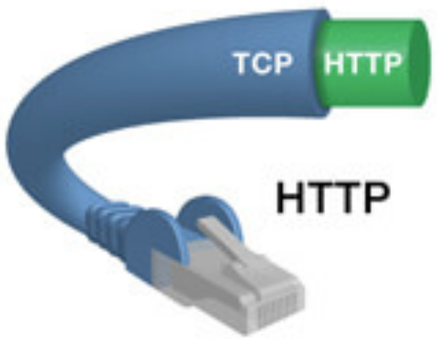
概述和握手过程

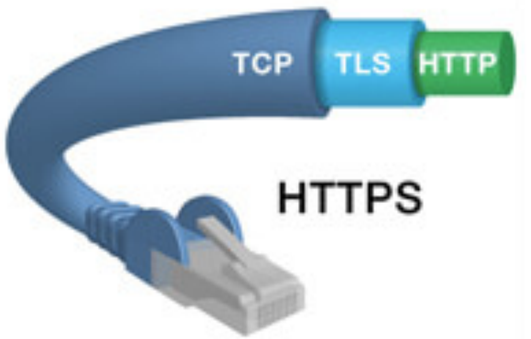
HTTP存在的问题

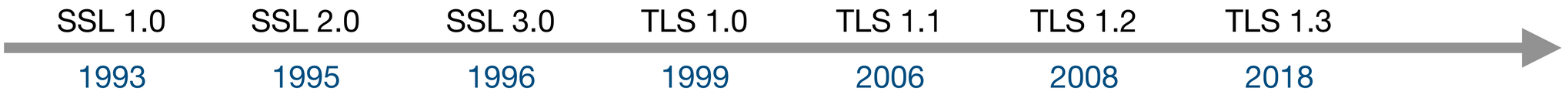
- 容易被监听
- 数据可能被篡改
- 容易假冒服务器

HTTPS

- HTTPS = HTTP over SSL
- SSL vs. TLS
  - SSL = Secure Sockets Layer 安全套接层
  - TLS = Transport Layer Security 传输层安全协议







加密算法

- 摘要　　MD5　SHA　　————验证数据未被篡改，不能防偷窥
- 对称加密　DES、3DES、RC-5、IDEA　　————加密解密密钥相同；加/解密速度快
- 非对称加密　RSA、ECC　　————加密解密密钥不同；加/解密速度慢

非对称加密：
私钥加密　——————　公钥解密
公钥加密　——————　私钥解密

数字签名：

对消息做摘要，用私钥加密摘要。密文即签名。签名同消息一起发送。

验证：
1、用同样算法对消息做摘要
2、用公钥解密密文
3、对比1和2的结果

对称加密和非对称加密比较

	加密/解密速度	密钥分发	使用范围
对称加密	快	难	大量数据加/解密
非对称加密	慢	易	极少量数据加解密

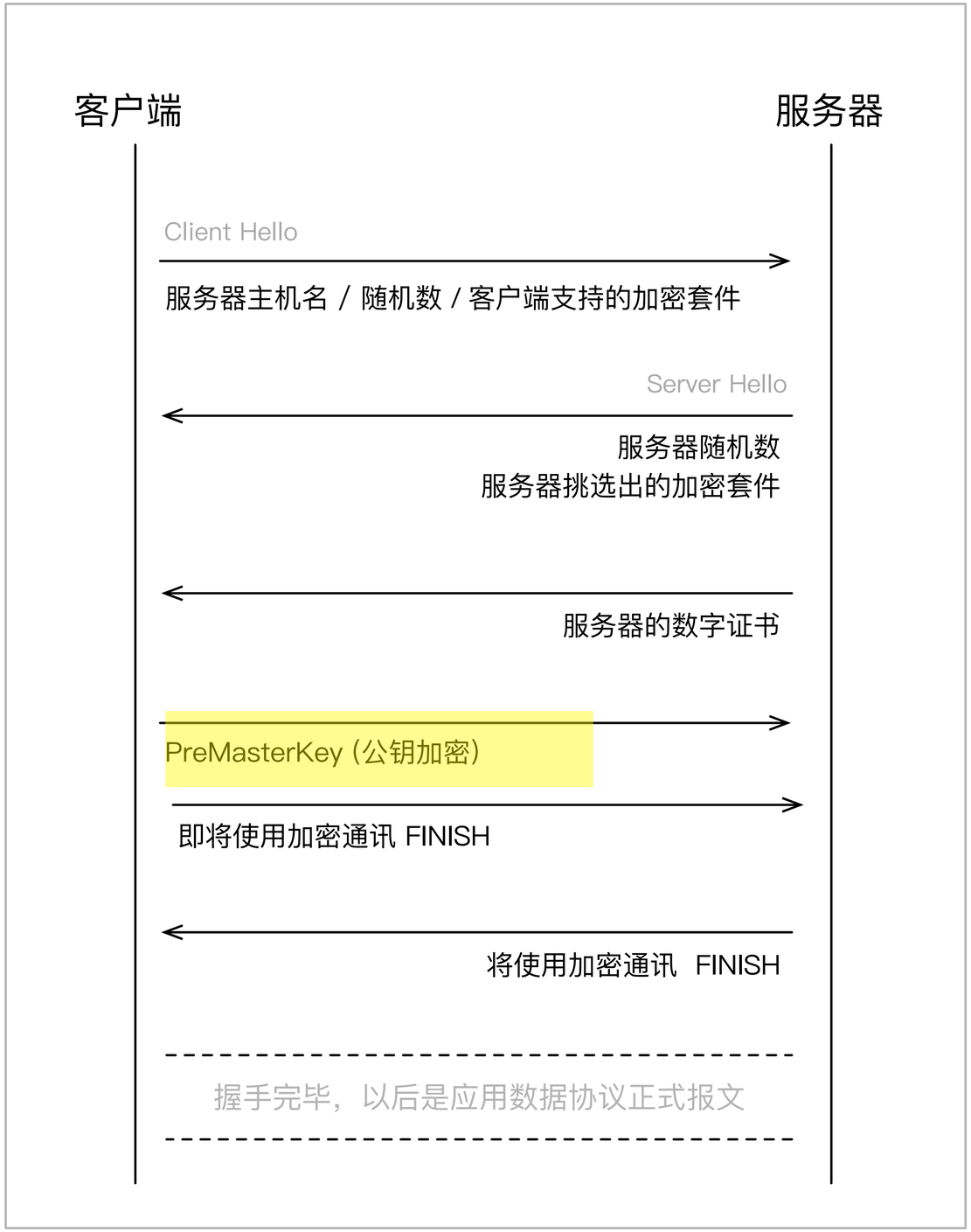
非对称加密传输密钥，对称加密传输数据；摘要算法保障数据完整

密码套件 Cipher Suite

密码套件的名称　例：TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

- 密钥交换算法，例如ECDHE_RSA，用于决定客户端与服务器之间在握手时如何建立通信，一般用非对称加密算法
- 批量加密算法，例如AES_128_GCM，用于加密消息流。一般是对称加密算法。
- 消息验证算法，例如SHA256，用于创建消息摘要，验证数据的完整性。

HTTPS连接过程



服务器数字证书

- 证书信息（域名、组织单位等）
- 有效期
- 证书公钥
- 证书签名算法
- 签发机构
- 数字签名（用签发机构私钥加密的证书数据摘要）