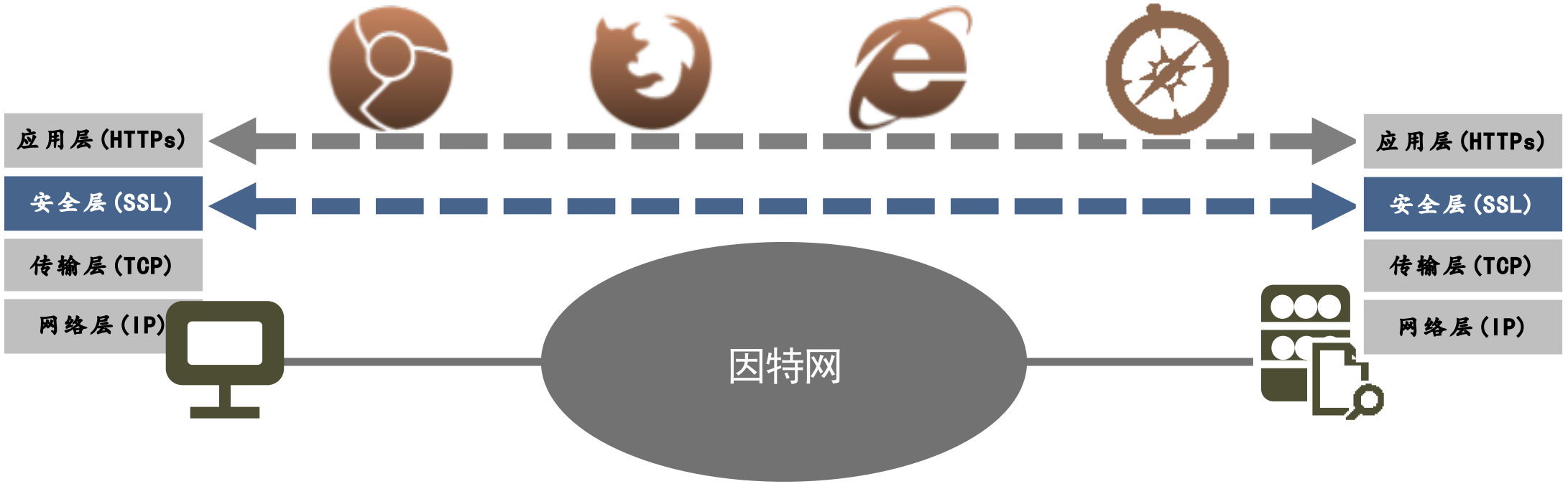
Secure Sockets Layer概述

安全的socket层

安全套接字层（SSL）：为网络通信提供安全及数据完整性的一种安全协议，SSL在传输层对网络连接进行加密。

RFC5246



SSL：Secure Sockets Layer

安全socket层功能

SSL支持多种算法和选项

- 是否使用压缩功能
- 使用哪些密码学算法
- 有哪些密码产品限制

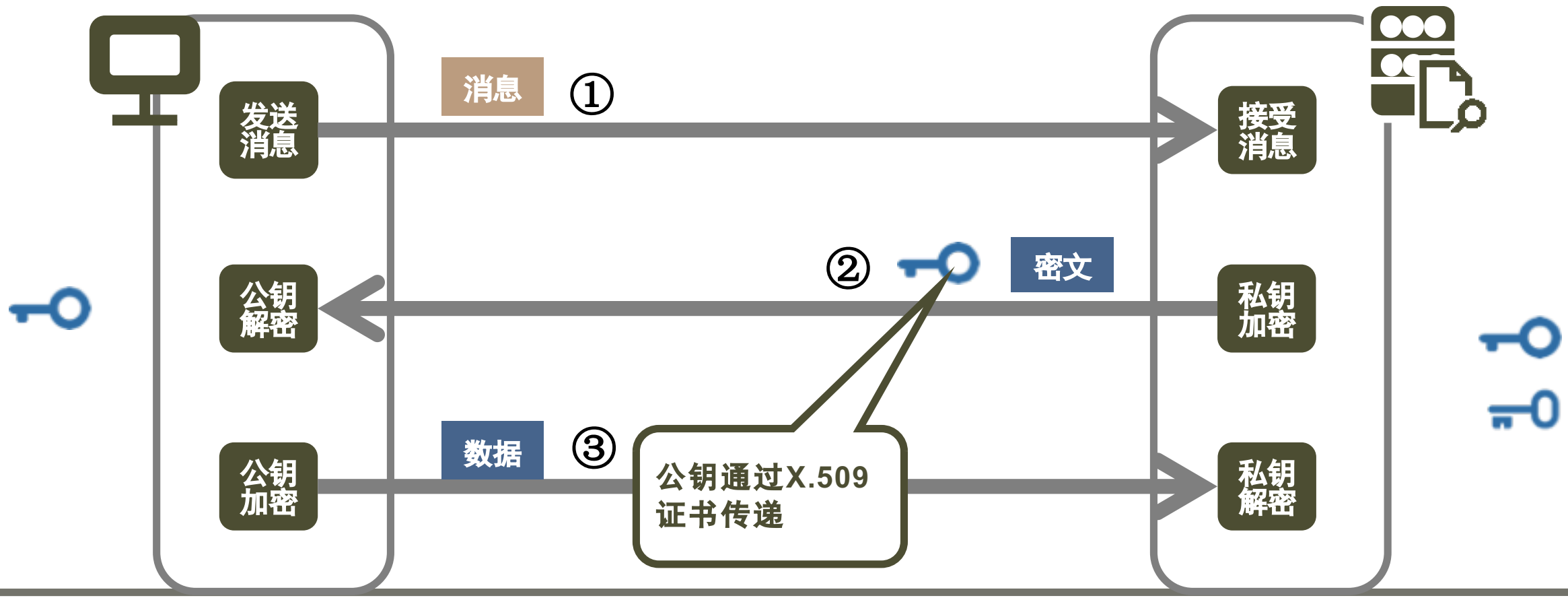
SSL功能

① 在两个socket之间建立安全连接
- 客户机与服务器参数协商
- 客户机和服务器双向认证
- 保密的通信
- 数据完整性

② 主要任务是压缩和加密

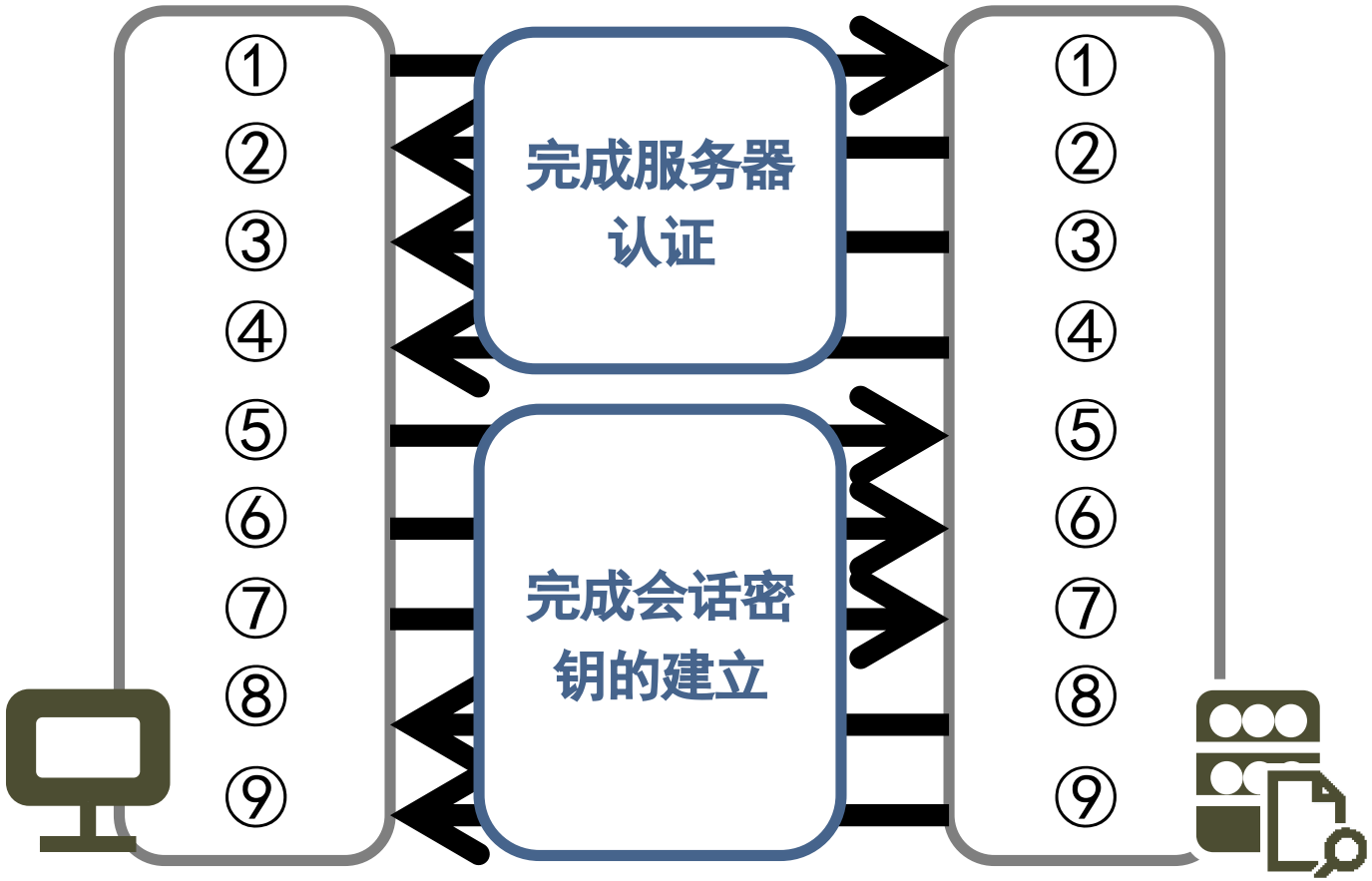
SSL的认证功能

- 一般公钥被包括在X.509证书
- 客户机会预装一些知名公钥



服务器公钥　服务器私钥

SSL连接的建立过程



客户机/服务器交互内容(/目的)
① SSL版本号,可选算法列表,临时值RA
② SSL版本号,选定的算法,临时值RB
③ X.509(服务器公钥)
④ 通知客户机消息
⑤ 用公钥加密的预设主密码
⑥ 通知服务器切换到会话密钥
⑦ 通知服务器客户机完成连接建立
⑧ 服务器切换到会话密钥
⑨ 服务器确认客户机

会话密钥的计算基于预设主密钥和两个临时值。

通过SSL传输消息

数据安全处理

- 待发送的消息被分割成长度为16KB的块
- 每块数据单独安全处理

- 消息认证码：利用协商好的散列算法进行散列运算获得
- 加密算法：采用连接建立过程中双方协商的算法
- 会话密钥：在连接建立过程中各自按照预设密钥和临时值计算