传输层安全

C5.1. 使用 SSL/TLS 时，为什么库不能自动知道要验证哪个服务器名称，而必须由应用程序明确提供？

C5.2. 书中所示的 `tls_client.py` 程序中，如果通用名检查失败，哪一行会失败？

C5.3. TLS 客户端与 TLS 服务器的主要区别是什么？只列出与 TLS 有关的差异。

C5.4. 在 Python TLS 服务器程序中，哪些调用完成下列操作？

(a) 发送服务器的证书，

(b) 要求服务器操作员输入保护服务器私钥的口令，

(c) 解密来自客户端的数据，

(d) 加密发送到客户端的数据。

C5.5. `example.com` 公司希望让 `www.example.com`、`mail.example.com`、`vpn.example.com` 等多台服务器共用一张证书，应如何做？

C5.6. 客户端程序通常用服务器证书认证服务器；服务器通常如何认证客户端？

C5.7. HTTPS 与 HTTP 有何关系？二者有什么共同点和区别？

C5.8. 浏览器访问 `https://www.example.com/getinfo.php` 时，服务器会执行 `getinfo.php`。那么在服务器端，谁负责建立 TLS 连接、与浏览器握手并提供服务器证书？是 `getinfo.php` 吗？

C5.9. 我们用 TLS 客户端程序访问 `https://www.facebook.com`，并希望出于调试目的在客户端与 Web 服务器之间部署 MITM 代理，使其可以查看甚至修改双方流量。不能修改客户端程序代码时，需要怎样配置客户端环境才能实现？