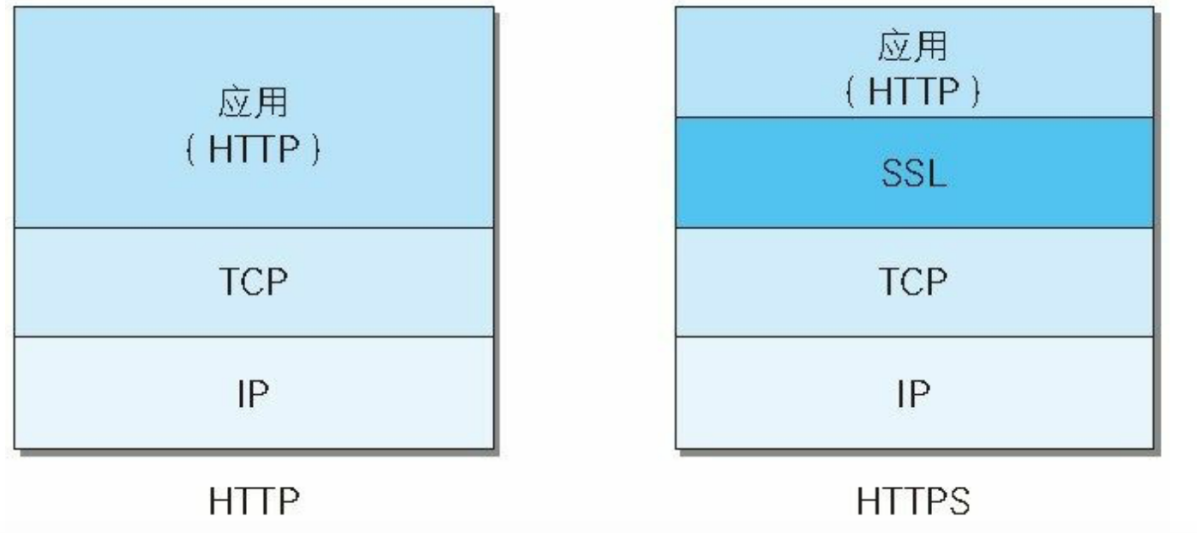
图解HTTP(7) 确保Web安全的 HTTPS（不是HTTP了！！）1

1 背景： HTTP存在 信息窃听【明文传输】、身份伪装【不进行身份验证？】等安全问题【无法验证报文的完整性，有可能被篡改】！

二、HTTPS【HTTP Secure 安全版HTTP】 = HTTP + 加密 + 认证 + 完整性保护 【这3重都是HTTP所缺失的】
1 HTTPS并非是 应用层的一种新协议！ 只是HTTP通信接口部分用 SSL 和 TLS 协议代替了而已！！！

2 可以看到，HTTPS是在 原先应用层中的HTTP 和 TCP之间加了一层 SSL【相当于加了SSL这一桥梁、中间人！！ SSL好像wei yu表示层吧？？】



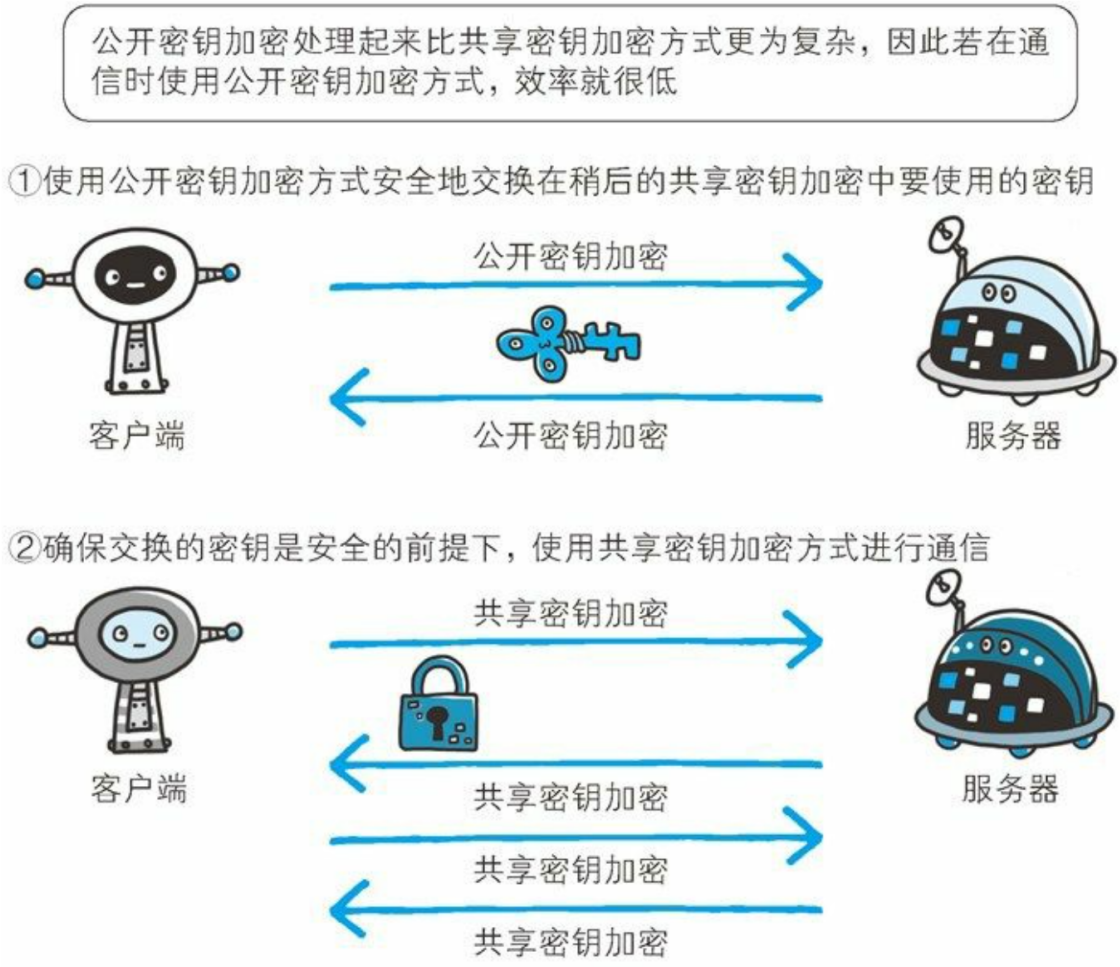
3 SSL不是为HTTP而生。
其他运行在 应用层【HTTP就属于应用层的】 的如 SMTP、Telnet 等均可与 SSL 配合使用！！
SSL是史上最为广泛使用的网络安全技术

4 对称加密。
加密 和 解密 都是用同一个密钥【“所以加密算法可以公开，就类似你家的锁 是公开的、暴露在外面，然后 钥匙就是私钥； 钥匙同时可以 开门、锁门！！ 但是别人一旦拿到你的私钥，那就随意进出了！！】

5 非对称加密【使用两把密钥的公开密钥加密】
一把称为私钥【不得让他人知道！】、一把公钥【可以随意转发出去】。
工作机制：
发送方用接收方的 公钥【公开的】进行加密，然后发送给 对方 ， 接着接收方用自己的 私钥

进行解密即可！！

5 HTTPS采用混合加密机制【汲取精华，但是有点看不懂其 工作机制、原理？？！】



完