1. 什么是https协议?

HTTPS并不是新协议, 只不过是让HTTP先和SSL通信, 让SSL再和TCP通信,

也就是说 HTTPS使用了隧道通信

1. https的作用:

通过使用SSL, HTTPS具有: 加密(防窃听), 认证(防伪装), 完整性保护(防篡改)

1. https的缺点:

1 因为有加密解密的过程, 所以速度会很慢

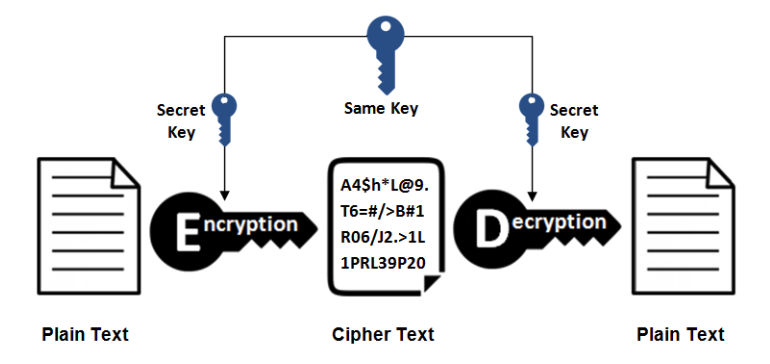
2 需要支付证书费用

1. https的加密有哪些?

1 对称秘钥加密 (Symmetric-Key Encryption): 加密解密用同一秘钥

优点: 运算速度快

缺点: 无法安全的将秘钥传给通信方



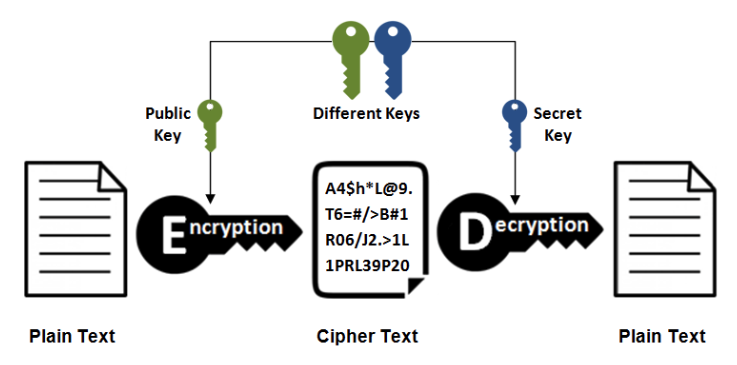
2 非对称秘钥加密 (Public-Key Encryption): 又称公开密钥加密, 加密解密使用不同的秘钥

公钥所有人都可以获得, 通信发送方获得接收方的公钥之后，就可以使用公钥进行加密，接收方收到通信内容后使用私钥解密, 非对称密钥除了用来加密

这个方法还可以用来进行签名, 因为私有密钥无法被其他人获取, 因此通信发送方使用其私有密钥进行签名, 通信接收方使用发送方的公开密钥对签名进行解密, 就能判断这个签名是否正确

优点: 更安全的将公钥传给通信方

缺点: 运算速度慢

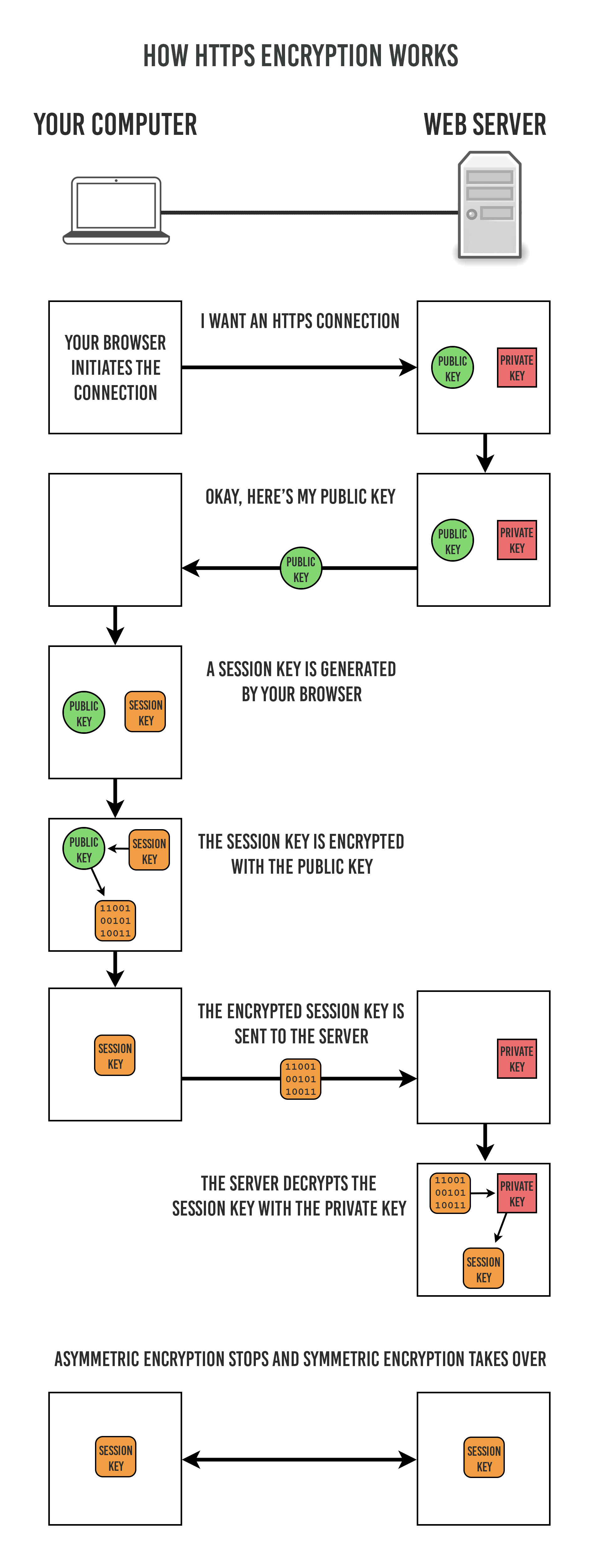


1. https是如何加密的?

https采用混合加密的方式, 使用非对称秘钥加密来传输对称秘钥, 保证秘钥传输过程的安全性,

使用对称秘钥加密通信来保证通信过程的效率

session key是对称秘钥



1. https的证书:

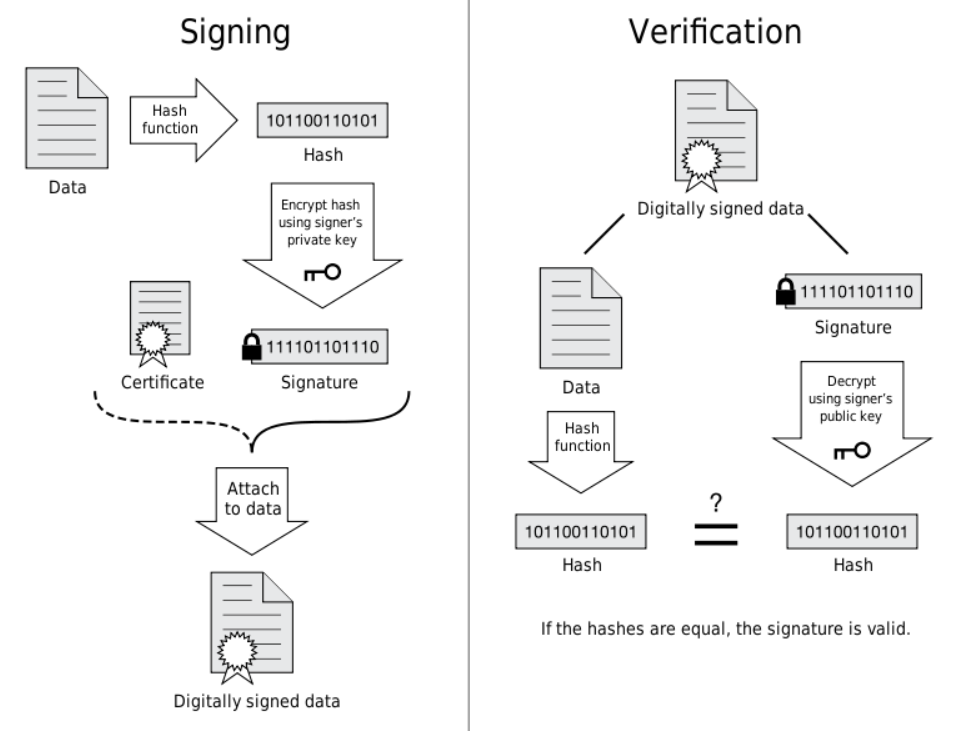
使用证书来对通信方进行认证

数字证书认证机构 CA (Certificate Authority), 是客户端和服务端都信赖的第三方机构

服务器的运营人员向CA 提出公钥申请, CA 判明身份后, 会对已申请的公钥做数字签名,

分配这个已签名的公钥, 并将公钥放入公钥证书中并绑定在一起

使用HTTPS通信, 服务器会把证书发送给客户端, 客户端获取到公钥后, 使用数字签名进行认 证, 如果认证成功就开始通信



1. http的完整性保护:

SSL提供了报文摘要来保护内容完整性

HTTP也有MD5内容摘要功能, 但是是不安全的, 当黑客对报文修改, 并且重新计算MD5的值 通信方是无法意识到被篡改的

HTTPS的内容摘要之所以安全, 是因为他结合了加密和认证两个操作, 加密之后的报文被篡改 后, 也很难计算出摘要, 因此无法轻易获得明文