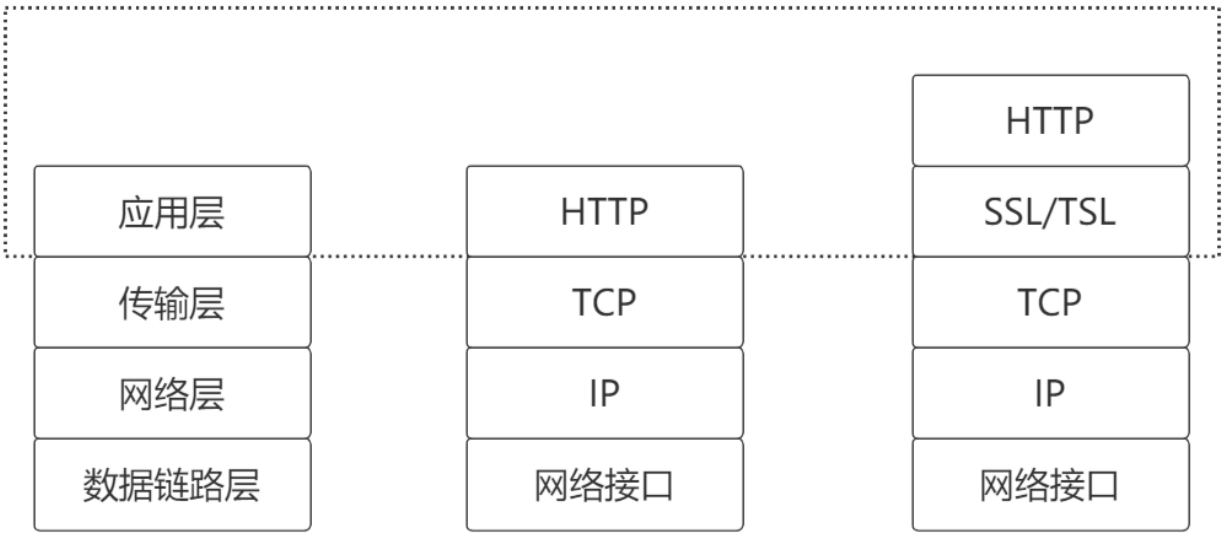
HTTPS协议

图灵学院
郭嘉

1. HTTPS

由于 HTTP 天生“明文”的特点，整个传输过程完全透明，任何人都能够在链路中截获、修改或者伪造请求 / 响应报文，数据不具有可信性。因此就诞生了为安全而生的HTTPS协议。

使用HTTPS时，所有的HTTP请求和响应在发送到网络之前，都要进行加密。

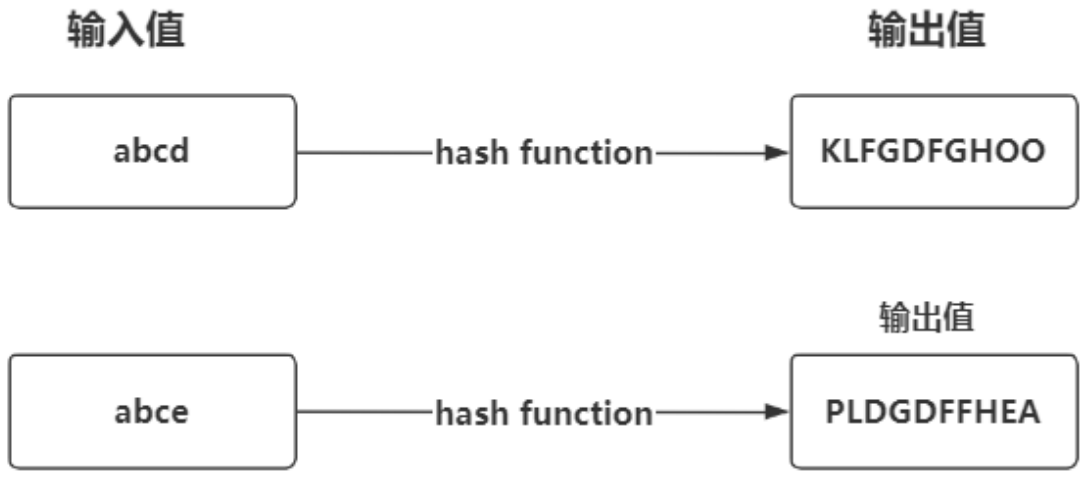


2. SSL/TLS

SSL 即安全套接层（Secure Sockets Layer），由网景公司于 1994 年发明，IETF 在 1999 年把它改名为 TLS（传输层安全，Transport Layer Security），正式标准化，到今天 TLS 已经发展出了主流的三个版本，分别是 2006 年的 1.1、2008 年的 1.2 ，2018的 1.3，每个新版本都紧跟密码学的发展和互联网的现状，持续强化安全和性能，已经成为了信息安全领域中的权威标准。

摘要算法

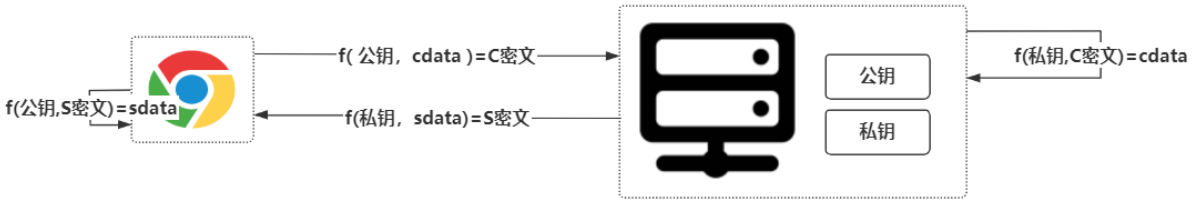
摘要算法能够把任意长度的数据“压缩”成固定长度、而且独一无二的“摘要”字符串，就好像是给这段数据生成了一个数字“指纹”。任意微小的数据差异，都可以生成完全不同的摘要。所以可以通过把明文信息的摘要和明文一起加密进行传输，数据传输到对方之后再进行解密，重新对数据进行摘要，再比对就能发现数据有没有被篡改。这样就保证了数据的完整性。



加密算法

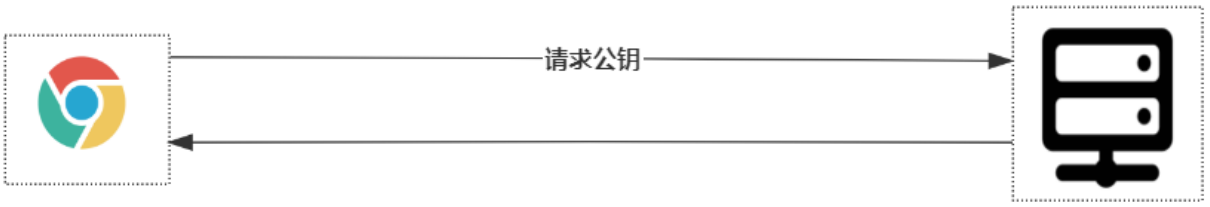
对称密钥加密算法：编、解码使用相同密钥的算法，如（AES，RC4,ChaCha20 ）。

非对称密钥加密算法：它有两个密钥，一个叫“公钥”，一个叫“私钥”。两个密钥是不同的，公钥可以公开给任何人使用，而私钥必须严格保密。非对称加密可以解决“密钥交换”的问题。网站秘密保管私钥，在网上任意分发公钥，你想要登录网站只要用公钥加密就行了，密文只能由私钥持有者才能解密。而黑客因为没有私钥，所以就无法破解密文。非对称密钥加密系统通常需要大量的数学运算，比较慢。如（DH、DSA、RSA、ECC ）

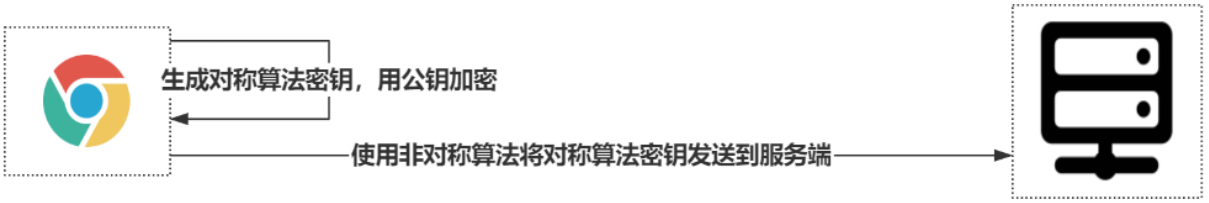


TLS 里使用的混合加密方式，即把对称加密和非对称加密结合起来呢，两者互相取长补短，即能高效地加密解密，又能安全地密钥交换。大致流程如下：

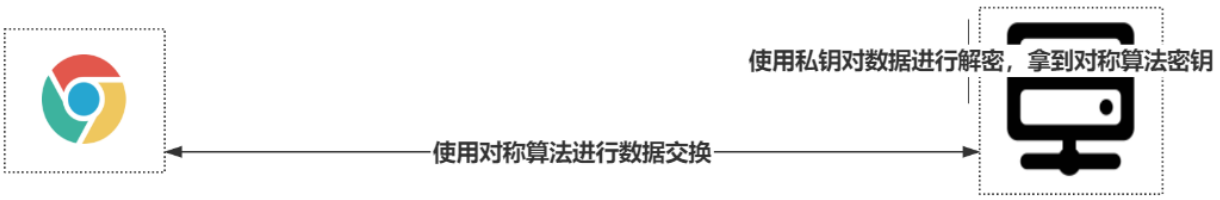
1.通信开始的时候使用非对称算法如 RSA,ECDHE先解决密钥交换的问题



2.用随机数产生对称算法使用的"会话密钥"，再用公钥加密。会话密钥很短，所以即便使用非对称加密算法也可以很快完成加解密。



3.对方拿到密文后用私钥解密，取出会话密钥。完成对称密钥的安全交换，后续就使用对称算法发完成数据交换



身份验证

数字证书组成：

CA信息，公钥用户信息，公钥，权威机构的签名，有效期

数字证书作用：

1.通过数字证书向浏览器证明身份

2.数字证书里面包含了公钥

数字证书的申请和验证

如何申请：

1. 生成自己的公钥和私钥，服务器自己保留私钥
2. 向CA机构提交公钥，公司，域名信息等待认证
3. CA机构通过线上，线下多种途径验证你提交信息的真实性，合法性
4. 信息审核通过，CA机构则会向你签发认证的数字证书，包含了公钥，组织信息，CA信息，有效时间，证书序列号，同时生成一个签名；

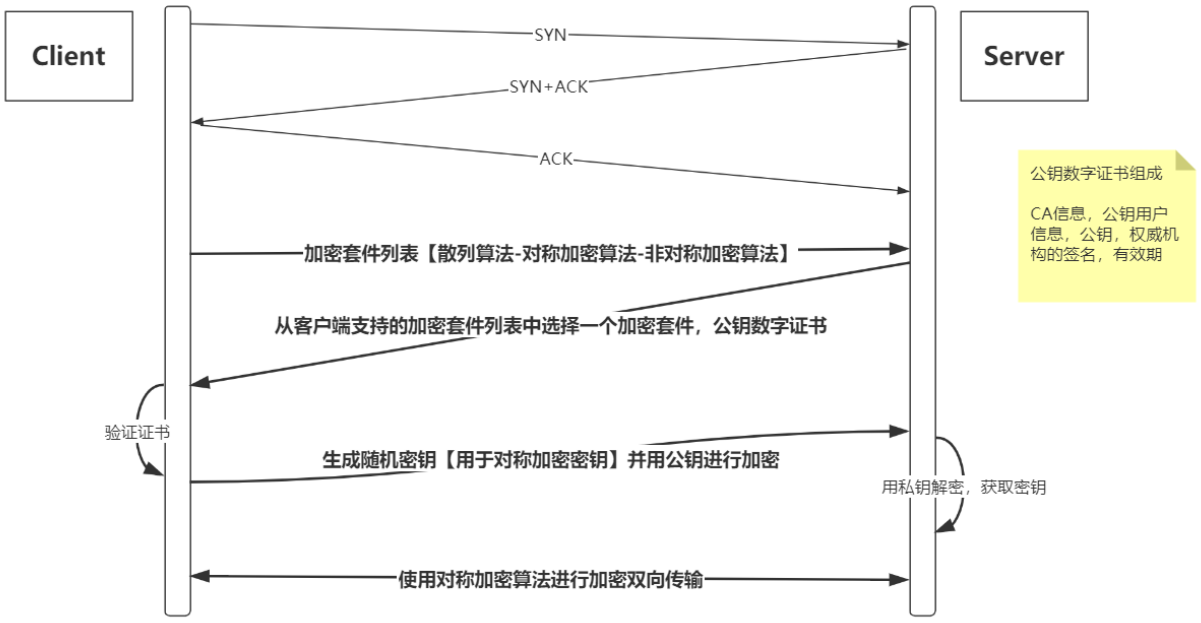
签名步骤: hash（ 你用于申请证书所提交的明文信息)=信息摘要；CA再使用私钥对 信息摘要进行加密，密文就是证书的数字签名

浏览器如何验证呢?

有了CA签名过的数字证书，当浏览器访问服务器时，服务器会返回数字证书给浏览器。浏览器收到证书后会对数字证书进行验证。

首先浏览器读取证书中相关的明文信息，采用CA签名时相同的hash函数计算得到信息摘要A，再利用对应的CA公钥解密数字签名数据得到信息摘要B，如果

摘要A和摘要B一致，则可以确认证书时合法的



知名的 CA 全世界就那么几家，比如 DigiCert、VeriSign、Entrust、Let’ s Encrypt 等，它们签发的证书分域名验证（domain validated,DV）证书、组织验证（organization validated,OV）证书、扩展验证（extended validation,EV）证书三种，区别在于可信程度。

DV可信级别是最低的，只是域名级别的可信，背后是谁不知道。
OV证书可信级别比DV高，会验证申请证书时填写的组织，企业信息是否是正确的，申请往往需要几天时间，
EV 是最高的，经过了法律和审计的严格核查，可以证明网站拥有者的身份。