

HenCoder Plus 讲义

HTTPS

備註：SSL 最初是由網景開發，僅用於 HTTP 加密通信（底層支持），但隨著發展，SSL 已經不僅用於加密 HTTP，因此，其名稱也由 SSL 更改為 TLS；事實上，TLS 也就只是分層，介於應用層（HTTP Layer）與傳輸層（TCP Layer）；簡單的說，就是在 HTTP 之下增加一個安全層。

定义

HTTP over SSL 的简称，即工作在 SSL（或 TLS）上的 HTTP。说白了就是加密通信的 HTTP。

SSL : Secure Socket Layer

TLS : Transport Layer Security

工作原理

備註：在初始階段使用非對稱加密協商出一套對稱加密的密鑰，爾後使用對稱對加密。

在客户端和服务端之间协商出一套对称密钥，每次发送信息之前将内容加密，收到之后解密，达到内容的加密传输

为什么不直接用非对称加密？

非对称加密由于使用了复杂的数学原理，因此计算相当复杂，如果完全使用非对称加密来加密通信内容，会严重影响网络通信的性能

HTTPS 连接建立的过程

1. Client Hello

2. Server Hello

3. 服务器证书 信任建立

4. Pre-master Secret

5. 客户端通知：将使用加密通信

6. 客户端发送：Finished

7. 服务器通知：将使用加密通信

8. 服务器发送：Finished

目的為將正確的「服務器公鑰（原數據）」傳送給客戶端。

再產生一個隨機數，並用服務器的公鑰加密後發送；而 Pre-master Secret 會與客戶端隨機數、服務器端隨機數，經過混合運算而產生 Master secret。

Master secret 又會再產生，客戶端加密密鑰、服務器端加密密鑰、客戶端 HMAC secret、服務端 MAC secret；MAC secret 為 hash-based message authenticate code，可以用來驗證身份且不能被公證驗證身份。

問題與討論：

問題一、為什麼「Master secret」是由「Pre-master secret」與「客戶端隨機數」、「服務器端隨機數」，這兩個未加密的數值混合運算後的產生，而不是單獨使用已經加密過「Pre-master secret」？

解答：其同樣是安全考量，例如避免「Replay attack」等。

問題二、為什麼後續還要產生「客戶端加密密鑰」與「服務器端加密密鑰」，請問與「非對稱加密」有關嗎？

解答：無關，在此處已經是使用「對稱加密」，只是客戶端發送信息時，會使用客戶端密鑰加密，而服務器端發送信息時，會使用服務器端密鑰加密，這是為了避免拿原消息回扔的攻擊。

问题和建议？

课上技术相关的问题，都可以去群里和大家讨论，对于比较通用的、有价值的问题，可以去我们的知识星球提问。

具体技术之外的问题和建议，都可以找丢物线（微信：diuwuxian），丢丢会为你解答技术以外的一切。



觉得好？

如果你觉得课程很棒，欢迎给我们好评呀！<https://ke.qq.com/comment/index.html?cid=381952>

一定要是你真的觉得好，再给我们好评。不要仅仅因为对扔物线的支持而好评（报名课程已经是你最大的支持了，再不够的话 B 站多来点三连我也很开心），另外我们也坚决不做好评返现等任何的交易。我们只希望，在课程对你有帮助的前提下，可以看到你温暖的评价。

更多内容：

- 网站：<https://hencoder.com>；<https://kaixue.io>
- 各大搜索引擎、微信公众号、微博、知乎、掘金、哔哩哔哩、YouTube、西瓜视频、抖音、快手、微视：统一账号「扔物线」，我会持续输出优质的技术内容，欢迎大家关注。
- 哔哩哔哩快捷传送门：<https://space.bilibili.com/27559447>

大家如果喜欢我们的课程，还请去扔物线的哔哩哔哩，帮我素质三连，感谢大家！

服務器證書，信任建立的詳細過程，其信息包含：

- 服務器公鑰（原數據）
服務器的主機名
服務器的地區
服務器證書的簽名

→ 為了避免「認證機構」攔截，並偽造信息，因此還必須去確認主機名（域名）。

- 證書簽發機構的證書
證書簽發機構的公鑰
證書簽發機構的名字
證書簽發機構的地區
證書簽發機構的證書的簽名

服務器公鑰（原數據）

經哈希後，以證書簽發機構的私鑰簽名後產生（並非原數據的服務器私鑰）。

服務器公鑰的簽名

為了確保服務器公鑰不是偽造的，需要「證書簽發機構的公鑰」來驗證。

以另一間證書簽發機構（根）的私鑰簽名。

證書簽發機構公鑰的簽名

用以驗證「證書簽發機構公鑰的簽名」的「另一間證書簽發機構（根）的公鑰」。

原則上，到了簽發機構的簽發機構的公鑰，也就是根證書機構，其可信性是可以查詢的，此外，作業系統中會有一張列表，其記錄著可信的簽發機構及根證書（用於確認簽名），但我們無法確認根證書是完全安全的，但我們也無法驗證，也就是說，我們只能相信它。