

HenCoder Plus 讲义

HTTPS

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。

工作原理

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

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。



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！