

Please visit website: <http://cxyroad.com>

严重威胁了网络通信的安全性。

![image.png](https://p1-juejin.byteimg.com/tos-cn-i-k3u1fbpfcp/bcc612213c8e4528aa1e4c546bad93d1~tplv-k3u1fbpfcp-jj-mark:3024:0:0:0:q75.awebp#?w=1555&h=770&s=424402&e=png&b=f6f5f5)

![image.png](https://p3-juejin.byteimg.com/tos-cn-i-k3u1fbpfcp/a2b6ea6db9fe40aebb516655f9f86bdd~tplv-k3u1fbpfcp-jj-mark:3024:0:0:0:q75.awebp#?w=46&h=205&s=400&e=png&b=f8f9fa)

![image.png](https://p1-juejin.byteimg.com/tos-cn-i-k3u1fbpfcp/382325b0663f4a62b176b38917fb5ef9~tplv-k3u1fbpfcp-jj-mark:3024:0:0:0:q75.awebp#?w=1458&h=765&s=295682&e=png&b=fffe)

3. HTTPS的加密机制

ge Cipher Spec`消息，告知服务器已准备好使用新的加密密钥进行通信。紧接着，浏览器会发送一个使用`master key`加密的`Finished`消息，以验证加密密钥的正确性。

7. 服务器在接收到这些消息后，也会进行相应的验证和处理。一旦验证通过，服务器会同样发送一个`Change Cipher Spec`消息和一个使用`master key`加密的`Finished`消息给浏览器，表示握手过程已完成，双方已建立起安全的通信通道。

8. 至此，HTTPS 的握手过程就告一段落了。

6. HTTPS的应用与推广

通过这个握手过程，客户端和服务端之间建立了一个安全的、加密的通信连接，为后续的数据传输提供了强有力的保障。这种通信方式不仅保证了数据的私密性和完整性，还能有效验证通信双方的身份，大大提高了网络通信的安全性。因此，HTTPS 协议在当今的网络通信中得到了广泛的应用和推广。

本文参考资料： [www.bilibili.com/video/BV1Ef...](http://cxyroad.com/"https://www.bilibili.com/video/BV1Ef4y1R7FW/")

原文链接: <https://juejin.cn/post/7352079398072713279>