HTTPS 初探

郭宁 @ 猫眼电影
guoning02@maoyan.com
2017/04/07

几个疑问

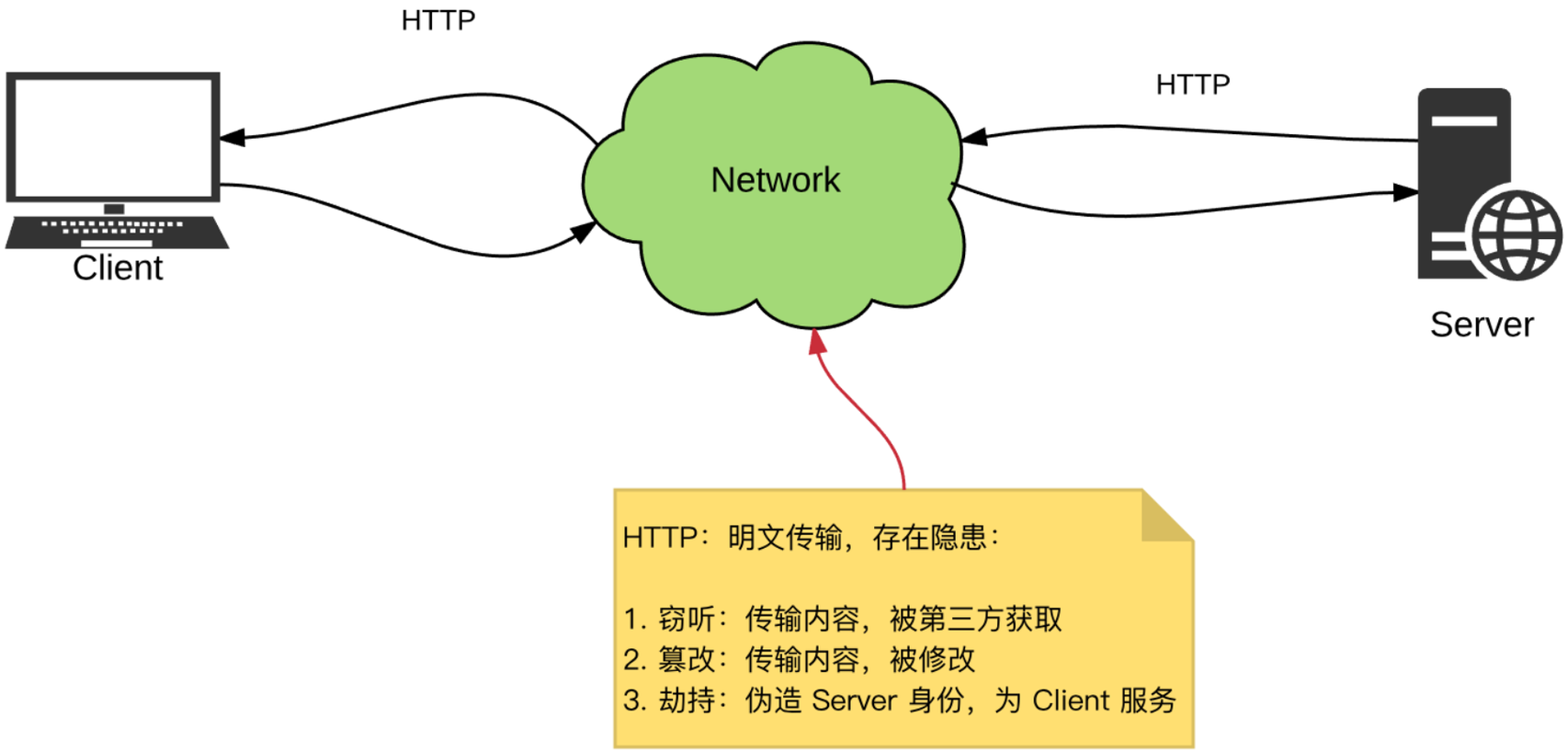
- **为什么**：
  - HTTP 应用这么多年，遇到什么问题了吗?
  - 为什么要升级到 HTTPS?
- **是什么**：
  - HTTPS 是什么?
  - 如何解决这些问题的?
- **怎么做**：
  - Web 服务，如何开启 HTTPS 支持?
  - 浏览器?
  - DNS?
  - Nginx 代理服务器?
- **代价**：
  - 引入 HTTPS 的收益？代价?

目录

HTTP 有什么问题?

- 问题一:
  - HTTP 应用这么多年，遇到什么问题了吗?
  - 为什么要升级到 HTTPS?

HTTP 有什么问题?



- **HTTP**，基于 TCP 的应用层协议，**明文传输**，存在隐患：
  - **窃听**：传输内容，被第三方获取
  - **篡改**：传输内容，被修改
  - **劫持**：伪造 Server 身份，为 Client 服务；又称：冒充、中间人攻击

HTTPS 能解决什么问题?

- **问题二:**

  - HTTPS 是什么?

  - 如何解决这些问题的?

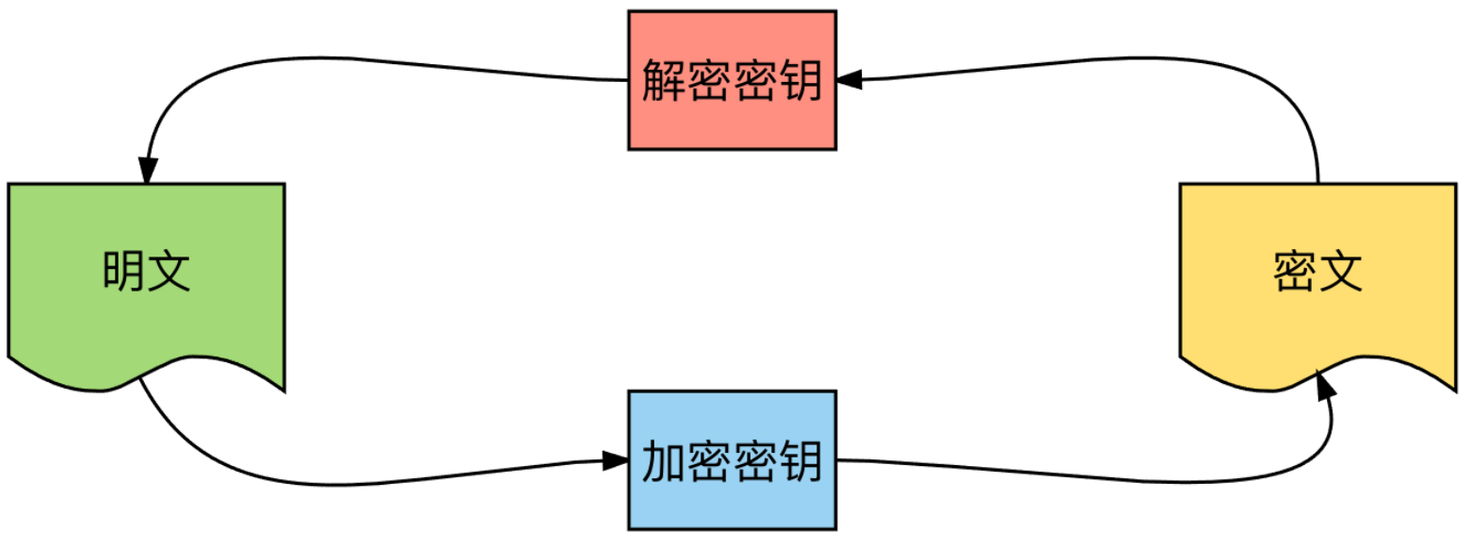
HTTPS 能解决什么问题?

- **有没有什么办法，解决上述问题?**
  - 归类一下，都是**安全性问题**，根源是「**明文传输**」
  - 怎么解决? **加密**。

- **加密，怎么加密?**
  - 加密、解密，需要**密钥**
  - **传递密钥**之前，是**明文传输**，此时，**如何传递**「密钥」?
  - 使用「**非对称加密**」，**传递**「对称加密」的「密钥」

补充：对称加密、非对称加密

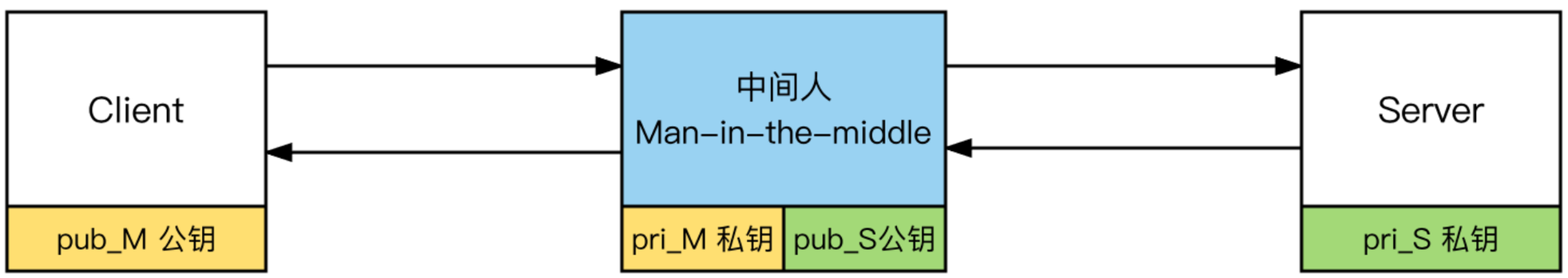
- **对称加密**：「**加密密钥**」**等于**「**解密密钥**」
- **非对称加密**：「**加密密钥**」**不等于**「**解密密钥**」
    - 「公钥」加密的内容，只有「私钥」能解密
    - 「私钥」加密的内容，只有「公钥」能解密
    - **非对称加密**，是**单向的**，**公钥**是**公开的**，任何人都可以获取公钥，从而获得 Server 信息的明文
- **非对称加密**的**典型作用**：**传递**对称加密的**密钥**



HTTPS 能解决什么问题?

- 思考:
  - 使用「非对称加密」+「对称加密」，能否解决所有安全问题? （窃听、篡改、劫持）

劫持：中间人攻击



- 风险仍然存在：「劫持」，中间人攻击（劫持）

HTTPS 能解决什么问题?

- 思考：
  - 使用「**非对称加密**」+「**对称加密**」，能否解决所有安全问题？（窃听、篡改、劫持）
- 解决办法：
  - 劫持，产生的根源：**无法验证**「**公钥**」**是否真的是指定网站所有**。
    - Client 如何验证「**公钥**」的有效性?
    - 引入**数字证书**，数字证书中包含公钥，只要证书是可信的，公钥就是可信的
    - 浏览器中，内置通用数字证书的验证逻辑和「根证书」

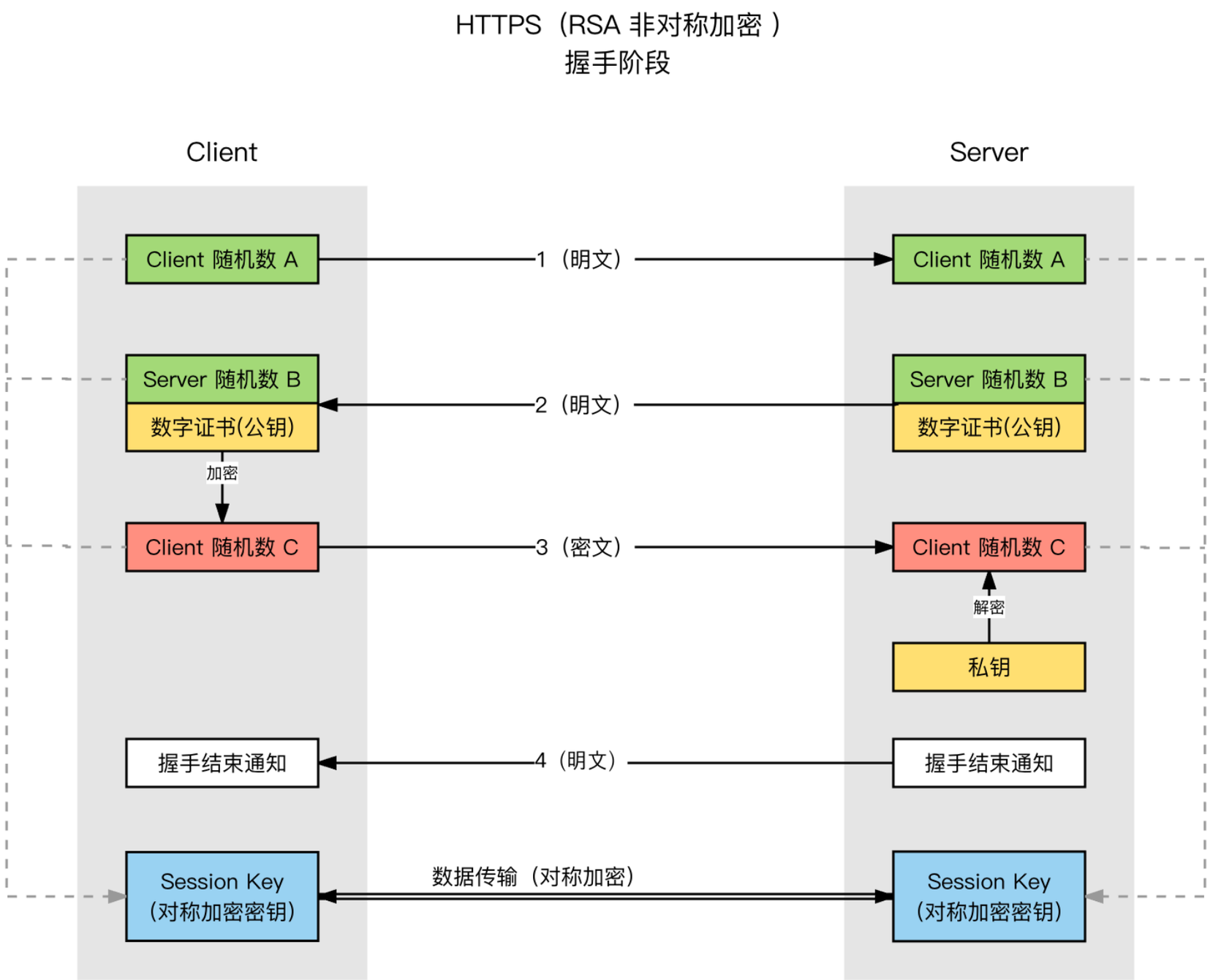
HTTPS 能解决什么问题?

- HTTPS 请求的连接建立过程:

    1. HTTP 是完全基于 TCP 协议的， TCP 是三次握手，建立的连接;

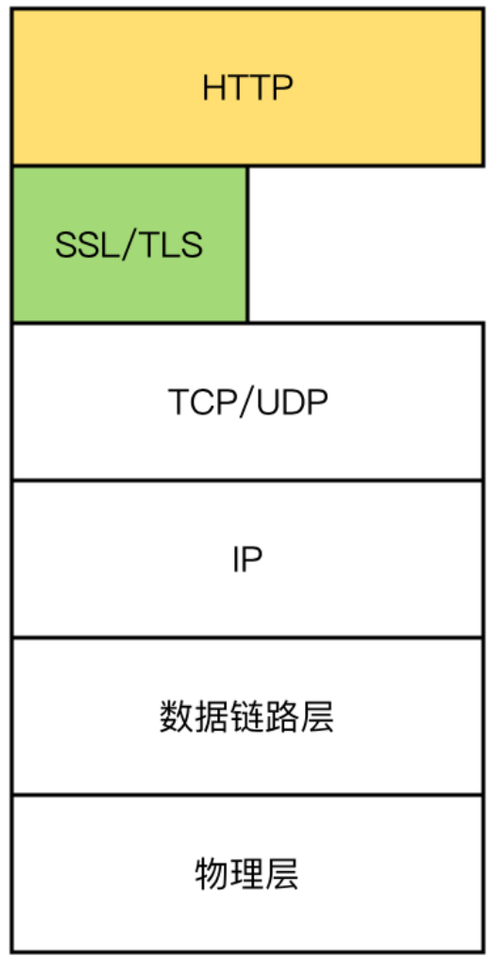
    2. HTTPS 请求，基于 SSL/TLS，连接是如何建立的?

HTTPS 能解决什么问题?



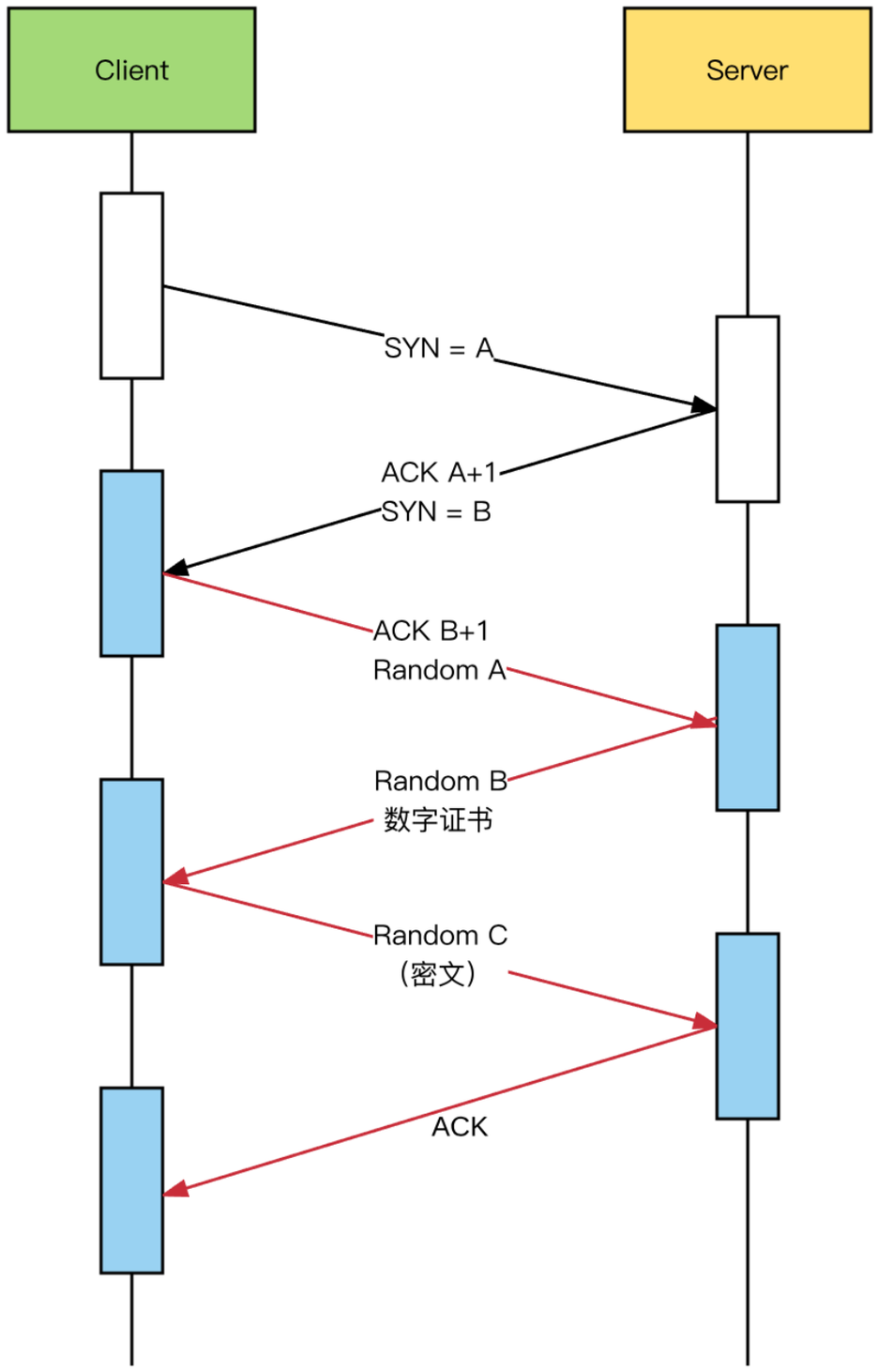
HTTPS 相对于 HTTP 有什么代价?

- 思考:
  - HTTPS 是否加密：HTTP Header 和 HTTP Body?



HTTPS 相对于 HTTP 有什么代价?

- HTTPS （HTTP over SSL/TLS）：
    - 使用 SSL 安全通道，非对称加密：交换随机数，生成对称加密的密钥；
    - 数据传输过程中：完整的 HTTP 协议，但使用密钥进行「对称加密」；
    - HTTPS 相对 HTTP ，获得了很好的安全性，那是否有代价呢?
        - 连接建立过程：增加了 SSL 的握手过程，连接建立时间，比 HTTP 要长 2～5 倍
        - 数据传输过程：HTTP 数据传输，需要加密、解密，时长更长
- HTTP vs. HTTPS：
    - HTTP耗时 = TCP握手
    - HTTPs耗时 = TCP握手 + SSL握手 （TCP 和 SSL 共用了一个请求）



HTTPS 说明：TCP + SSL

1. SSL 握手，需要 2 个 RTT（Round-Trip Time，往返时间）