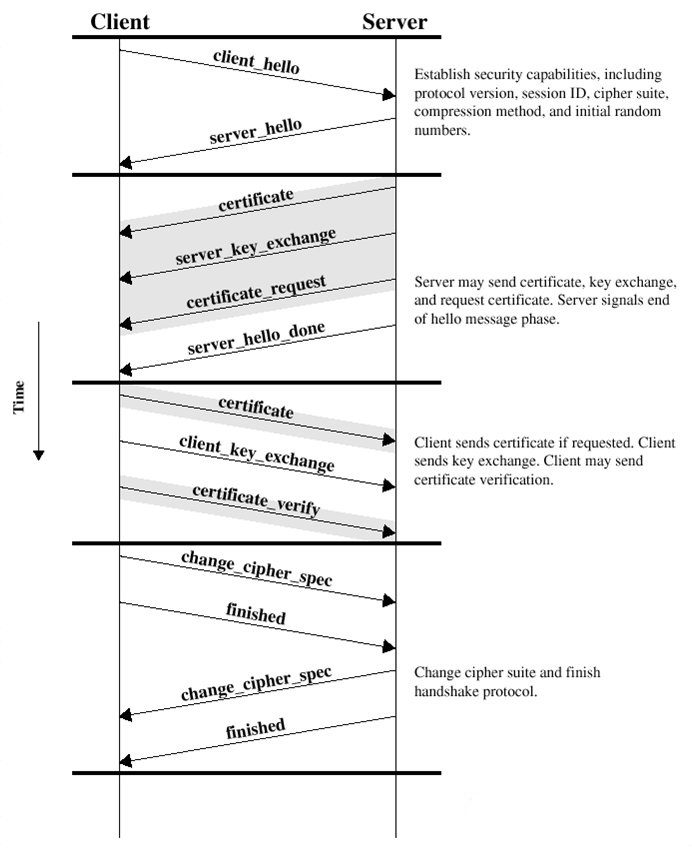
**TLS项目**

**本项目的目标**

首先对TLS过程和最新的TLS1.3进行了简单的模拟实现。通过这个项目，您将对TLS有一个很好的理解。如果您感兴趣，您可以进一步研究TLS协议草案RFC8446。**（参考）**



**这些项目应该实现些什么**

该项目应包括两部分：客户端和服务器

.

1. 客户端和服务器应该设置一个连接以相互通信。你可以通过套接字来实现这一点。
2. 客户端和服务器应就加密的会话密钥达成一致，会话密钥应显示在服务器的屏幕或用户界面上。注：会话密钥主要由客户端决定。

一种简单的方法如下：

首先，客户端生成会话密钥，然后使用服务器的公钥，客户端加密会话密钥并将其发送到服务器

非常感谢您想更好的方法进行会话密钥生产。

1. 客户端加密一个字符串，计算MAC并将它们发送给服务器
2. 服务器解密，验证MAC。

**建议**

1. 字符串加密方法应该是对称的，如DES、3DES，这比非对称的要快得多。
2. 您可以使用SHA-256来计算MAC。

**你应该交什么**

1.必须包含一个详细的设计文档，同时如何生成会话密钥。

2.源代码

3.可执行程序和手册

**高质量的编程**

请注意代码的质量。你可以简要地介绍和讨论心脏出血(<https://heartbleed.com/>)在你的报告。

**这个项目将于10月10日开始。一直持续到11月26日。16.**

您必须将所有文件（代码、设计文档、可执行程序）压缩为a。zip文件，文件名是学生号码和名字的组合。例如，“192053017-你的名字”。zip“。

**程序工具**

您可以使用一些依赖于用于实现的编程语言的TLS库。这些库包括许多DES、MD5等算法。你应该使用它们而不写欠款级的密码。

**警告：你自己去做吧。**

**你的分数是什么组成**

可执行程序的正确性： 60%

客户端和服务器连接的比例为15%

会话关键生产15%

加密朊病毒和解密15%

MAC并验证15%

文档和源代码的可读性： 40%

设计文件： 15%

手册： 10%

源代码： 15%

在会话密钥生产之前，客户端和服务器可以相互通信，就加密、MAC等算法达成一致。约定的算法应显示在客户端的屏幕或用户界面上

**参考资料：**

您可以参考RFC8446<https://datatracker.ietf.org/doc/rfc8446/>