什么是非对称加密?

非对称加密（也称为公钥加密）使HTTPS协议成为可能。非对称加密使用两个密钥而不是一个。

学习目标

阅读本文后，您将能够：

- 了解什么是非对称加密
- 了解非对称和对称加密之间的区别
- 解释为什么非对称加密对于TLS / SSL协议很重要

相关内容

- **公钥加密**
- **SSL 如何运作**
- **SSL 握手**
- **什么是 SSL 证书?**
- **Keyless SSL**

复制文章链接

什么是非对称加密?

加密通信有两个方面：加密数据的发送方和解密的接收方。顾名思义，非对称加密在每一方都是不同的。发送者和接收者使用两个不同的密钥。非对称加密，也称为公钥加密，使用公钥加私钥：用公钥加密的数据只能用私钥解密。

TLS（或 SSL）是让 HTTPS 成为可能的加密协议，它部分依赖于非对称加密。客户端将从该网站的 TLS 证书（或 SSL 证书）获得网站的公钥，并使用该公钥来发起安全通信。该网站则秘密保存私钥。

什么是对称加密?

在对称加密中，同一密钥既可以加密也可以解密数据。为了使对称加密有效，两个或多个通信方必须知道密钥是什么。为了保持安全，任何第三方都无法猜测或盗取密钥。

TLS/SSL如何使用非对称加密和对称加密?

TLS，过去称为 SSL，是一种用于加密网络通信的协议。TLS 使用非对称加密和对称加密。在 TLS 握手期间，客户端和服务器就用于对称加密的新密钥达成一致，称为“会话密钥”。每个新的通信会话都将以新的 TLS 握手开始并使用新的会话密钥。

TLS 握手本身使用非对称加密来保证安全，同时双方生成会话密钥，以验证网站源服务器的身份。

加密密钥如何工作?

密钥是一串数据，与加密算法结合使用时，可以对消息进行加密或解密。使用密钥加密的数据看起来像一系列随机字符，但任何拥有正确密钥的人都可以将其恢复为明文形式。（密钥也可用于对数据进行数字签名，而不仅仅是加密。）

Cloudflare如何帮助网络属性部署非对称加密?

Cloudflare 提供免费 SSL/TLS 证书以供使用。已注册 Cloudflare 的网站所有者可以一键实施 SSL/TLS。这让网站能够轻松地从 HTTP 迁移到 HTTPS，保持用户数据安全并增加用户信任。

要了解有关 SSL/TLS 握手以及它们如何使用非对称和对称加密的更多信息，请参阅 TLS 握手中会发生什么?