

关于 n1Crypto 的介绍

· 简介

在通讯安全越来越不能保障的今天。常用的那些即时通讯软件（如 QQ 微信等）已经显然不能满足通信安全的需求。为了解决这个问题，可以通过 XMPP、TELEGRAM 等即时通讯方式来通信。但是由于各种原因，比如 XMPP 学习难度高。TG 需要手机号 VPN 等问题导致可能无法广泛使用。因此可以使用 n1Crypto 这样的折中实现方案来临时解决在不安全的即时通讯软件上进行较安全通信的问题。

n1Crypto 是 GitHub 上一个开源的通信加密项目 (github.com/muHua-usnnrqffjcqv/n1Crypto)。支持类似 HTTPS/XMPP/PGP 的端对端加密，也支持对称加密。并且加密的结果有一定的伪装性。能运用到 QQ 等不安全的通信渠道。加密效果如下：

ne ita vero primus si de primus sum is uter fio amo ad cur do iam vos an
quoque diu amo ob pater si nos pars sui vix que sic ita aliquis umquam annus
nam fio inquam que sui vir uter vel aut XD

混淆的效果甚至能使用百度翻译进行翻译(当然, 翻译出来的不是加密的原文)
效果：“我若活在肉身上，这是我劳碌所得的。我要向你们怎样行呢？我也要为父怎样行，我们若活在肉身上，这是我生命的结果。”

可见，除了文本可能比较长以外，混淆效果还是可以的。

该加解密算法使用 AES 进行加密并进行 n1b 混淆，理论上如果密码不泄露的话，安全性可以保障。目前该软件只支持电脑（WIN）。

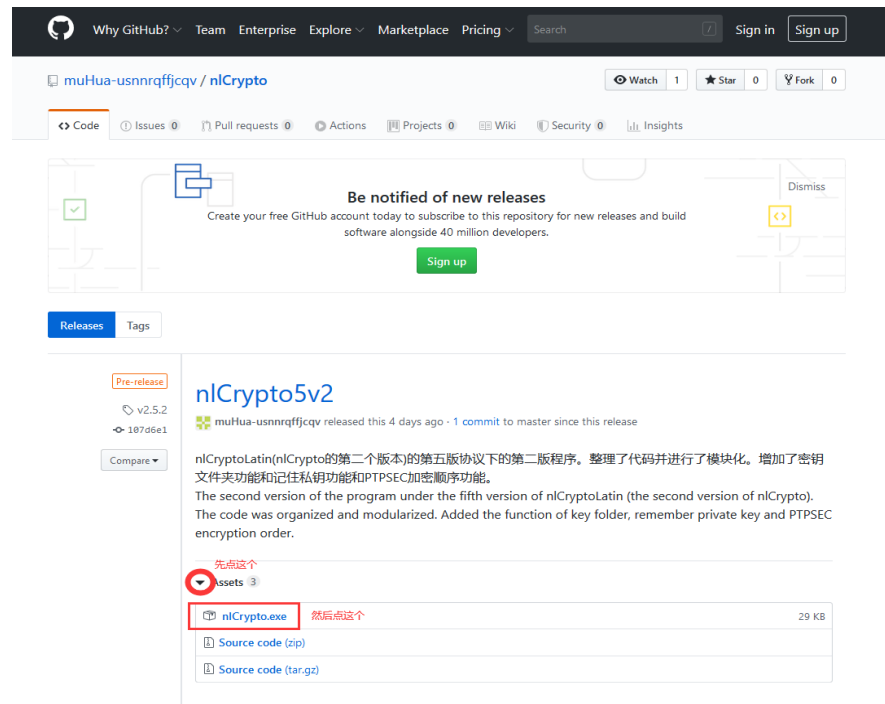
获取方式

可以从该软件的 GitHub 发布页下载软件。这是网页：


<https://github.com/muHua-usnnrqffjcqv/nlCrypto/releases>

下载方法请见右图：

1. 点击最上面版本的 ASSET 的左面的三角号
2. 点击 nlCrypto.exe 下载



使用方法

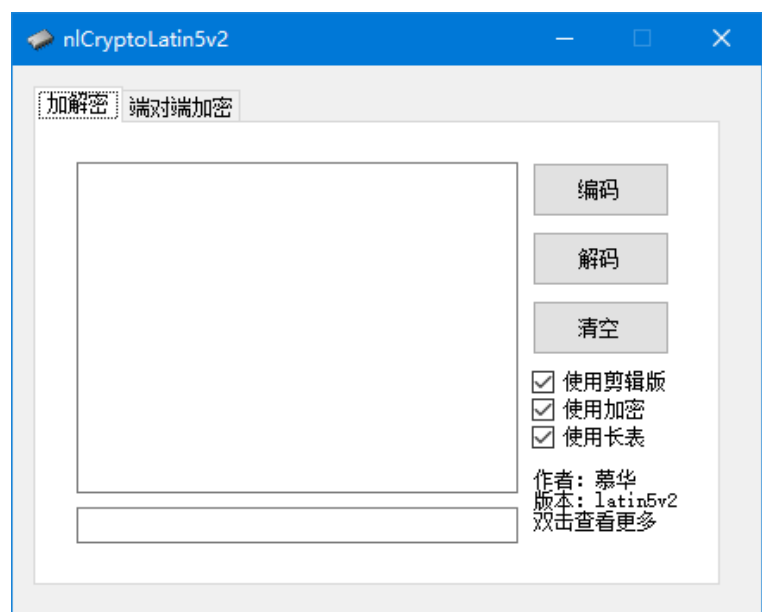
下载之后会有这个程序： **nlCrypto.exe**。由于是单程序应用。因此可以直接放到桌面上。或者您也可以放到 ProgramFiles 或个人文件夹中。

放好位置之后，双击即可打开程序。页面大概会类似右图。如果您使用的版本更新的话页面可能会有些区别，但应该是没有太大区别的。

普通加解密

普通加解密使用的是对

称加密的 AES 算法。如果密钥不泄露的话，安全性比较可靠。如果您讨论的不是



特别需要安全加密的内容, 或您讨论的对象或您自己认为端对端加密的难度过大。

建议使用普通加密法。

主页面左下角的输入框是密码输入框。您可以在其他场合（比如线下，线上也可以用一些暗号）进行约定。

左上角的输入框是内容输入框，您可以将需要加密的内容或需要解密的内容输入进行加解密。

使用剪辑版的选项勾选（默认）的情况下，您切换到程序的时候剪贴板的内容会自动粘贴到内容输入框中。加密完毕的时候加密后的文本也会自动复制到剪辑版中。比较方便配合即时通讯软件使用。

使用加密和使用长表您暂且可以不用管，因为用处不大。

加密

在密码输入框中输入约定的密码，在内容输入框中输入文本。然后点编码即可加密。结果会在内容输入框中。此时就可以将文本粘贴到即时通讯软件中了(如果您是配合即时通讯软件使用的话)。

解密

在密码输入框中输入约定的密码。在内容输入框中粘贴密文。然后点解码即可解密。结果会在内容输入框中。

端对端加解密

普通的对称加密有个致命缺陷：如果只在线上通讯的话，密码安全不能保障。比如假如我使用的 QQ，我需要向你发送一份加密信息。这就有问题了，我该如何向你发送密码呢？如果直接明文给你发送的话显然是可能会被截获的。传统的解决方法是线下传递密码。另一种解决方法是密码为某个问题的答案：比如“我

是什么年份出生的”这种。如果不能够线下传递、并且安全性需要提高呢？这就可以使用端对端加密来进行通信。端对端加密的算法基于 RSA 和 AES 的类 PGP 加密法。理论上安全性是比 AES 的对称加密高些的。并且端对端加密的密钥可以用来确认身份。



右图是端对端加密的页面。从普通加密的页面点上面的端对端加密选项卡即可打开。

公私钥生成

端对端加密首先需要准备公私钥。这里可以点公私钥生成按钮来生成（注：该软件不支持 PGP 或 X.509 公私钥(因为作者懒)）。生成之后会自动放在您个人文件夹的下面的 keys 文件夹。位置：%userprofile%\Keys

您应当把私钥（即 privateKey.xml）保管好。不要让任何他人获得。并且您应当将公钥（即 public.xml）分发给任何您可能以后需要加密通讯的人。

同时生成的公钥和私钥是相互绑定的。

另外，他人给你发的公钥文件建议改成您对其的称呼并放在%userprofile%\Keys\下（通讯时方便查找）。

注：如果您已经有某个人的公钥的情况下，他想要给你发送新的公钥（并且两个公钥不同）的情况下，请仔细检验（比如询问他人或询问一些问题等）。有可能该人的身份就不是之前您通讯的对象了。（当然，也可能确实是对方遗失了

公私钥)。

开始一次端对端加密通信

在您和您需要通信的对象都已经生成了公私钥并且双方都有了双方的公钥的情况下。就可以开始加密通讯了。

点击“选择您的私钥”按钮，选择您的私钥。(在新版本，如果私钥没有变动的話，只需要第一次选择一次即可。)

然后点击“选择您讨论对象的公钥”按钮，选择您讨论对象的公钥。

点击“临时通讯密钥生成”按钮，并且将您的临时通讯密钥发给对方。对方也生成。然后互相交换临时通讯密钥，点击解码。

然后您就可以点会普通加解密页面进行加解密了。临时通讯密钥框里是双方同用的解码后的临时通讯密钥。

端对端加密还有什么好处

您在进行端对端加密通讯的时候，能完全确定您通讯的对象确实是当时给你发送公钥的人（如果对方没有泄露私钥的话）。并且在通讯完成之后。如果不同时有双方的私钥的话，这段对话理论上是无法解密的。因此端对端加密有类似阅后即焚的功能和对方身份得确定的功能。

群聊的端对端加密

由于工程量可能比较大，本版本（nlCryptoLatin5v2(v2.5.2)）还没搞。因此莫得教程。可以等之后的版本。

· 结语

上述就是 nlCrypto 的教程。

本教程采用 CC-BY-SA 4.0 即：知识共享-署名-相同方式共享 进行发布。

本教程最新版可见 <https://github.com/muHua-usnnrqffjcqv/nlCrypto> 中的
“about”文件夹和 <https://github.com/muHua-usnnrqffjcqv/nlCrypto/wiki> 中。

如果程序有 BUG 或者您使用有疑惑可以在 <https://github.com/muHua-usnnrqffjcqv/nlCrypto/issues> 开个 ISSUE。

2020 年 4 月 27 日 muHua 制作