本站使用**PGP/GPG**加密技术保护联系表单

Published on Jul 12, 2022 UTC by Wang Ye <https://wangye.org>

我的网站老访客可能会有印象，之前的联系表单是支持PGP/GPG加密正文的，后来使用ASP.NET重构后这一部分实现始终存在问题，判断可能是第三方库的BUG，一直没有再加上这个功能，最近该第三方库进行了升级，发现这个BUG已经修复了，于是在联系表单启用了PGP/GPG加密特性。

1 什么是**PGP/GPG**

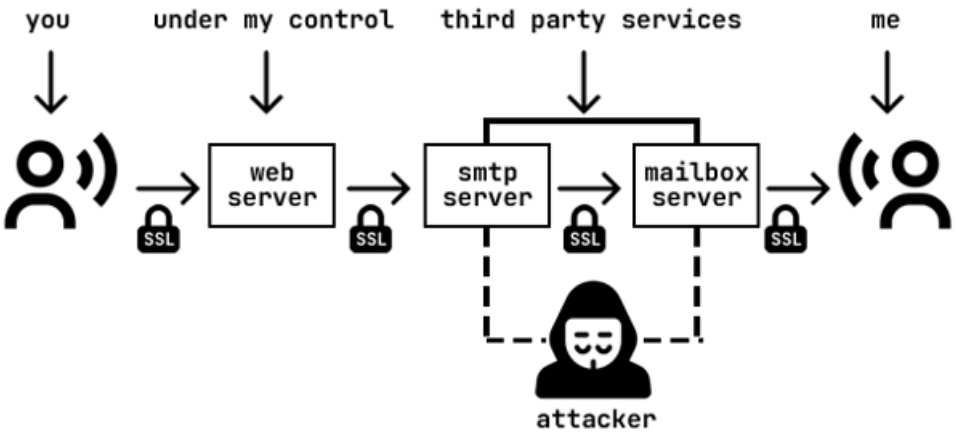
PGP/GPG虽然是两种写法，但实际上是一种东西，首先我们要介绍PGP（Pretty Good Privacy），这是一套消息加密、验证的技术，由一系列散列、数据压缩、对称密钥加密，以及公钥加密的算法组合而成，最早由菲利普·齐默曼（Philip R. Zimmermann）发明并应用于电子邮件安全隐私保障，可以这么说在没有PGP和TLS加密的时代电子邮件或多或少的在互联网上明文裸奔，而且被篡改的几率很大。PGP最初由Philip免费在互联网上发布，但其本人也因此违反了美国政府关于加密软件出口的限制而受到刑事调查，美国政府的打击并未影响到PGP成为世界上受欢迎的邮件安全隐私保障技术之一，后来Philip成立了商业公司运营PGP，PGP也成为一种事实上的标准（OpenPGP, RFC4880）。

GPG（GNU Privacy Guard）又称GnuPG，是OpenPGP标准的开源自由软件实现，绝大多数的开源技术在涉及PGP技术都使用了这个实现，同样本站也是依赖于此实现了PGP加密功能。

2 为什么要加密邮件正文

本站联系表单通过电子邮件方式传输信息，这依赖于第三方邮件发送方和本人的电子邮箱服务商所提供的服务，虽然访客与本站的连接的通过HTTPS/TLS加密的，并且本站与第三方邮件发送方也使用了TLS加密传输通道，但是仍然无法确保第三方邮件发送方和本人电子邮箱服务商无法窥探到所发送的信息，所以如果发送的信息十

分敏感，这需要用到PGP/GPG加密，这样邮件正文将会被安全加密，实际上如果网友通过联系表单或者电子邮件咨询问题或者与我唠嗑则可以不加密邮件正文，加密与否在于邮件信息的敏感性和泄漏带来的危害。



3 联系表单如何加密邮件正文

本站联系表单为了降低网友使用门槛，特地将加密功能进行了集成，也就是说在发送联系表单之前勾选使用PGP/GPG加密选项，那么Web应用将在后台加密要传输的正文内容，并且将密文交由SMTP服务器发送至我的邮箱服务器，我本人在特定终端下载密文后使用Yubikey解密获取原文，当然我公开了PGP/GPG的公钥，大家也可以自行加密并将密文贴至联系表单的正文文本框（这时就不要再勾选使用PGP/GPG加密复选框了）。

当然由Web直接运算PGP/GPG加密还有一点小隐患，那就是如果本人的Web服务器被攻击者控制，那么消息正文将在加密前被获知，虽然这种情况极为罕见（本人漏洞补丁打的很勤），但如果不放心那还是使用我公开的PGP/GPG公钥手动加密后在密文发送吧。

目前此加密功能还处于实验阶段，另外需要提醒的是本人为确保安全一般在特定设备上读取加密信息，如果阁下选择加密那么相应的邮件处理将不会那么及时，还请理解。

External References (Links)

公开了PGP/GPG的公钥
https://wangye.org/publickey.asc