发布后，有人把 PGP 放到了因特网上，美国以外的外国人也可以下载它。在美国，加密程序分类为军用品，依据联邦法律不得出口到国外。

尽管缺乏资金，没有收入，也没有公司的支持，还要受到政府的干预，但 PGP 还是成为了世界上广泛使用的电子邮件加密软件。奇怪的是，因为 Zimmermann 案件，美国政府无意中促进了 PGP 的传播。

美国政府在 1996 年初放弃了这个案子。这一声明得到了许多因特网团体的喝彩。Zimmermann 案件已经成为无辜的个人为了自己的权益反抗强大的政府滥用职权的历史。政府的让步是值得庆幸的事，部分原因是由于在国会中对因特网审查制度的游说，以及 FBI 推动允许越来越多的政府侦听。

在政府撤案后，Zimmermann 建立了 PGP 公司，该公司于 1997 年 12 月并入网络联盟（Network Associates）。Zimmermann 现在是密码学领域中一位独立咨询者。

8.5.2 PGP

Philip Zimmermann 于 1991 年所写的 **PGP**（Pretty Good Privacy）是一个电子邮件加密方案，如今已经成为一个事实上的标准。其 Web 站点以每个月百万页的规模，为在 166 个国家的用户提供服务［PGPI 2012］。在公共领域中有各种版本的 PGP 可供使用；例如，你能够在国际 PGP 的主页上为你喜爱的平台找到 PGP 软件以及许多有趣的读物［PGPI 2012］。（特别是 PGP 作者所撰写的一篇特别有趣的文章［Zimmermann 2012］。）PGP 的设计在本质上和图 8-21 中所示的设计相同。PGP 软件的不同版本使用 MD5 或使用 SHA 来计算报文摘要；使用 CAST、三重 DES 或 IDEA 进行对称密钥加密；使用 RSA 进行公开密钥加密。

安装 PGP 时，软件为用户产生一个公开密钥对。该公钥能被张贴到用户的网站上或放置在某台公钥服务器上。私钥则使用用户口令进行保护。用户每次访问私钥时都要输入这个口令。PGP 允许用户选择是否对报文进行数字签名、加密报文，或同时进行数字签名和加密。图 8-22 显示了一个 PGP 签名的报文。这个报文在 MIME 首部之后出现。报文中的加密数据为 $K_A^-(H(m))$，即数字签名的报文摘要。如我们上述讨论，Bob 为了验证报文的完整性，需要得到 Alice 的公钥。

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash:  SHA1
Bob:
Can I see you tonight?
Passionately yours, Alice
-----BEGIN PGP SIGNATURE-----
Version: PGP for Personal Privacy 5.0
Charset:  noconv
yhHJRHhGJGhgg/12EpJ+lo8gE4vB3mqJhFEvZP9t6n7G6m5Gw2
-----END PGP SIGNATURE-----
```

图 8-22　PGP 签名报文

图 8-23 显示了一个秘密 PGP 报文。这个报文也出现在 MIME 首部之后。当然，明文报文不包括在这个秘密电子邮件报文中。当一个发送方（例如 Alice）要确保机密性和完整性时，PGP 在如图 8-23 所示的报文中包含一个类似于图 8-22 中的报文。