RSA

 $Crazy_13754$

2024年1月14日

摘要

写了些关于 rsa 的东西

目录

1 引言 2 过程 3 awa 3

1 引言

网上找到的博客质量参差不齐。实际上,写这篇的时候发现有论文写的很清楚了^[1]。此外维基百科也写的非常好,本来把它们丢上来就可以了。你问我为什么还要写这篇文章?请看这个图 1:



图 1: This is an inserted jpg graphic

如果你还是没有明白我想说什么,请再看看这个表 1:

对写奇奇怪怪东西的看法	可以理解	不可理喻
支持	0.1%	0.0%
不支持	0.2%	99.7%

表 1: Table to test captions and labels

如果(虽然几乎是当然的)你还是不理解,那就看看这些东西:









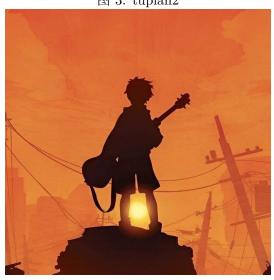


图 4: tupian3

图 5: tupian4

这显然把事情弄得更糟。好吧,只是我在学 L^AT_EX,而你浪费了不少时间来看刚刚的内容。而且你接下来看到的东西也会几乎全是复制的。

公钥密码系统的观点是由 Diffie 和 Hell man 在 1796 年首次提出的,它是密码学发展史上具有 里程碑意义的一件大事。与传统对称密码体制 (即加、解密密钥相同) 相比,公钥系统使用两个密钥: 加密密钥可以公开,称为公钥;解密密钥保密,为私钥。产生公钥体制的内在动力有两个:

- (1) 传统对称体制下密钥的存储和分配问题;
- (2) 消息鉴别问题, 就是指用来检验消息来自于声称的来源并且没有被修改。

公钥体制的基础是陷门 (单向函数), 即某种实际处理过程的不可逆性。目前的公钥思想基于两种: 一是依赖于大数的因数分解的困难性; 二是依赖于求模 p 离散对数的困难性。RSA 密码算法就是基于大数的因数分解的困难性。

2 过程

3 证明

rsa 的证明。

参考文献

[1] 陈传波 and 祝中涛. Rsa 算法应用及实现细节. 计算机工程与科学, 28(9):13-14, 2006.