email:79996286@qq.com

hthf

< 2019年7月 >

日	一	二	三	四	五	六
30	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31	1	2	3
4	5	6	7	8	9	10

公告

昵称：hthf
园龄：5年2个月
粉丝：2
关注：0
+加关注

搜索

找找看
谷歌搜索

常用链接

我的随笔
我的评论
我的参与
最新评论
我的标签

我的标签

linux for x84(1)

随笔分类(15)

ibm power linux(1)
ibm小型机(2)
linux for x86(5)
oracle error(3)
存储(1)
杂项(3)

随笔档案(15)

2016年2月 (1)
2015年11月 (1)
2014年8月 (4)
2014年7月 (2)
2014年6月 (2)
2014年5月 (5)

阅读排行榜

1. 我理解的数字证书-1-公钥，私钥和数字证书(11557)
2. linux下使用parted工具划分大于2T的分区(2114)
3. 日立HDS AMS2100存储的调试(1906)

我理解的数字证书-1-公钥，私钥和数字证书

英文原文地址：

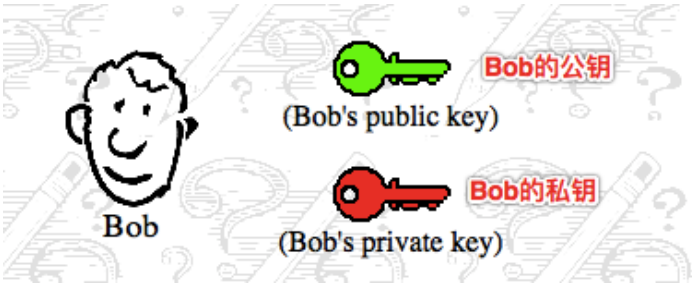
http://www.youdzone.com/signature.html

若下文有任何错误，请告知我，谢谢。79996286@qq.com

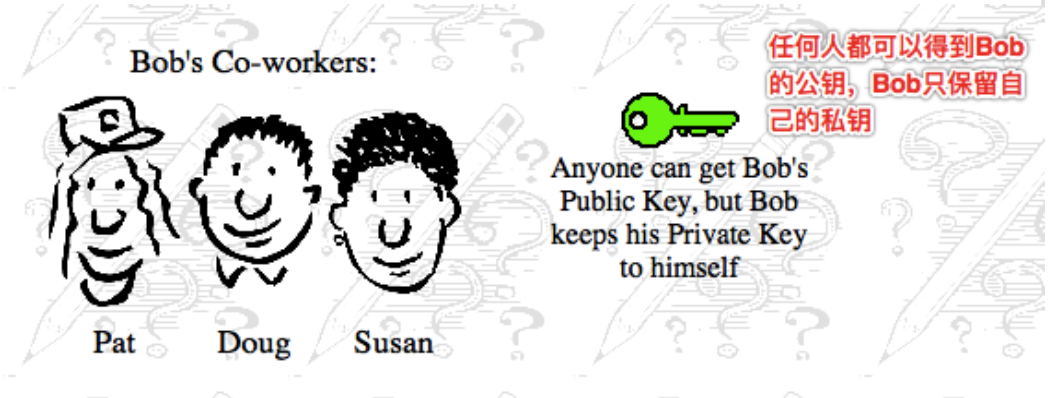
主角介绍：Bob and Alice

提起RSA加密算法，公钥和私钥，多数文章都要使用Bob和Alice这两位人物。他们的创造者名叫Rivest，是RSA之父。他为了在避免在描述中使用A和B，就以这两个字母开头，创建一男一女两个角色，就是我们在任何文章上都能看到的Alice和Bob了。这是一些题外话，下面就来进入我们的数字证书入门学习吧。

什么是数字证书



Bob有两把钥匙，一把叫公钥（public key），一把叫私钥（private key）。

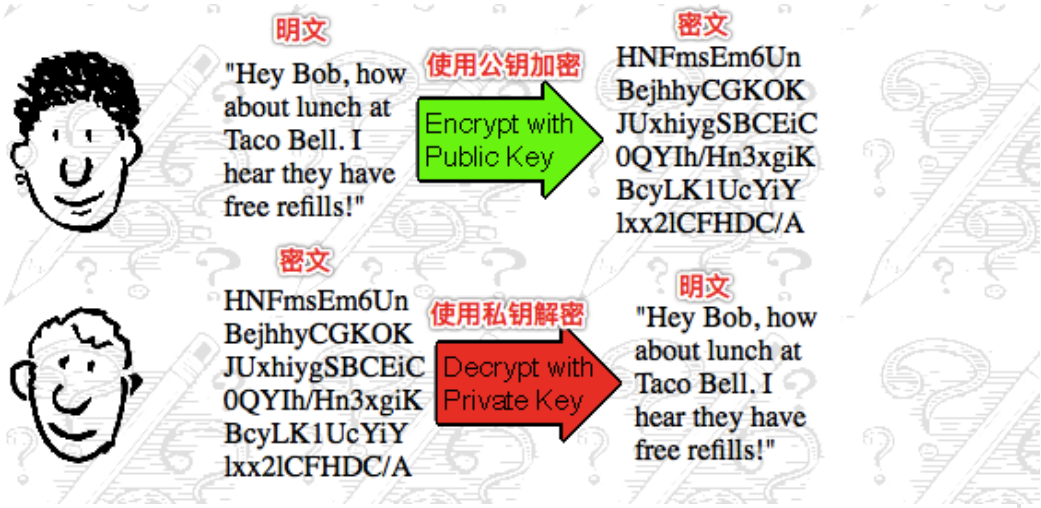


Bob的公钥可以公开供其他人使用，他只保留自己的私钥。公钥和私钥用来加解密数据，如果使用任意一把来加密数据，那么只有使用另外一把才能解密数据。

4. oracle11.2.0.3.0 RAC aix7100-02-02-1316 crs-4124,crs-4000错误问题解决(781)
5. 解决BEA-000438 Unable to load performance pack.(546)

推荐排行榜

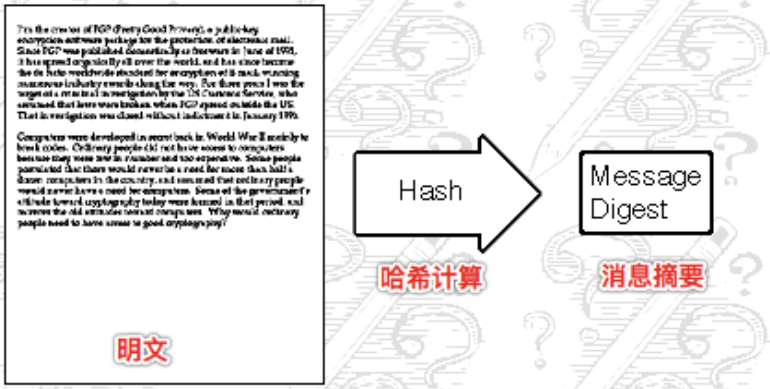
1. 我理解的数字证书-1-公钥，私钥和数字证书(4)



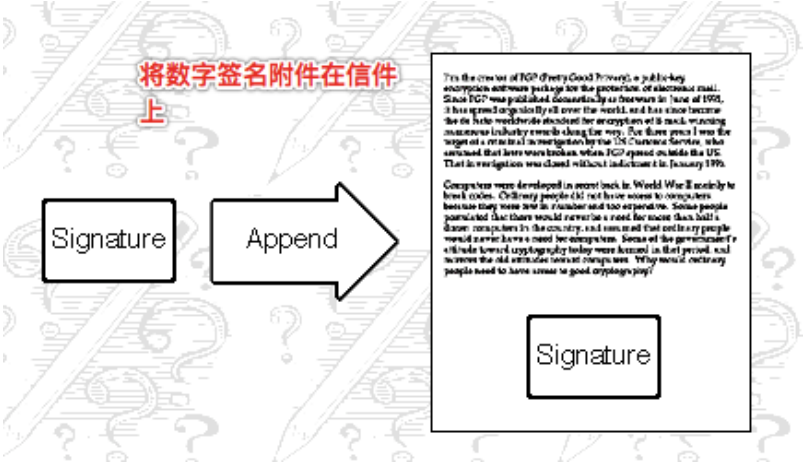
Susan想给Bob写信，她可以使用Bob的公钥将内容加密以后发送给Bob，Bob收到以后，使用私钥解密以便阅读内容。Bob的的其他同事即使截获了Susan发送给Bob的信件，由于没有Bob的私钥，也无法解密，从而确保数据安全。以上就是使用公钥和私钥加解密的过程演示。

多说一句，如果Bob给Susan回信，如何保证数据安全呢？他可以使用Susan的公钥加密消息后发给Susan，Susan使用自己的私钥解密后阅读。所以保护好自己的私钥是多么重要的事情啊。

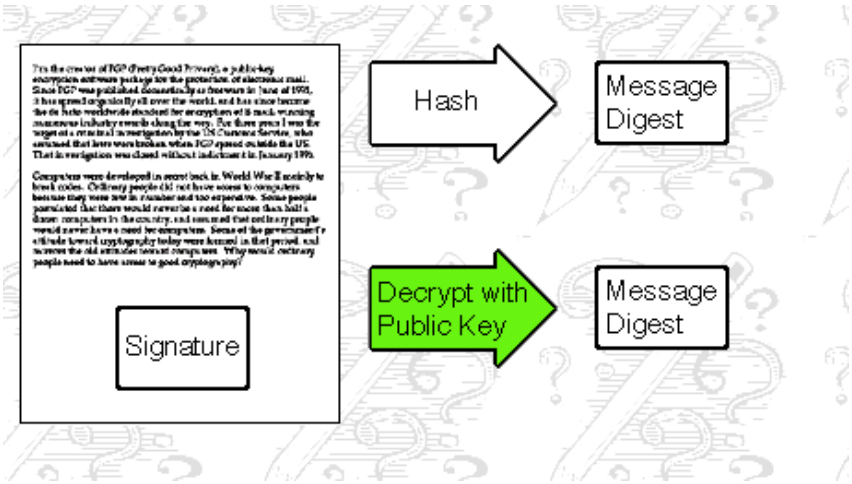
现在Bob决定给Pat写一份信，信件的内容不用加密，但是要保证Pat收到信件后，能够确认信件的确是Bob发出的，而不是别人冒充Bob发给Pat的，应该如果做呢？



Bob将信件通过hash软件计算一下，得到一串消息摘要（有的文章也称之为"hash值"）。这一过程能够保证2点：1、过程不可逆。即不能通过消息摘计算出信件的内容。2、消息摘要不会重复。即如果信件有任何改动，再次hash计算出的消息摘要一定不会和改动前的消息摘要一致。



然后，Bob使用自己的私钥，将消息摘要加密。加密后的结果，我们称之为“数字签名”。现在，Bob就可以将信件连同数字签名一起发给Pat。



Pat收到信件以后，会做2件事：1、使用Bob的公钥将数字签名解密，如果顺利解密，说明的确是Bob签发的数字签名，不是别人签发的，因为Bob的私钥没有公开。2、Pat使用hash软件对信件再次进行hash计算，和解密数字签名得到的消息摘要对比，如果一致，说明信件没有篡改，确实是Bob发出的。这就是数字签名的过程。它能够确保签名人发出的消息不被篡改，也能证明的确是签名人发出的消息。

ok，一切看上去是那么的完美，使用公钥私钥，即能加解密消息，又可以数字签名。说了那么多，还没有提到文章的主题----数字证书（不要和数字签名搞混了）。

先来做一道CISP的试题：

那类人对单位的信息安全威胁最大：a、高层领导　b、信息主管　c、安全管理员　d、心怀不满的员工

三长一短选最短，三短一长选最长，so答案就是d，也是我们下面引入的主角，Doug，our disgruntled employee。

Doug要欺骗Pat，冒充Bob给Pat写信，他应该怎么做的？既然Bob的公钥是公开的，Doug可以冒充Bob，将他自己的公钥发给Pat，让Pat误认为收到的公钥就是Bob的，然后就可以冒充Bob给Pat发消息了（这里我们只谈理论，不谈具体实现方式）。所以问题的核心就是，如何确保公钥不被冒充?

使用数字证书可以确保公钥不被冒充。数字证书是经过权威机构（CA）认证的公钥，通过查看数字证书，可以知道该证书是由那家权威机构签发的，证书使用人的信息，使用人的公钥。它有以下特点：

1、由专门的机构签发的数字证书才安全有效。

2、签发数字证书是收费的。

3、不会被冒充，安全可信。

4、数字证书有使用期限，过了使用期限，证书变为不可用。CA也可以在试用期内，对证书进行作废操作。

5、CA的公钥已经集成到操作系统中了。如上图。

生成数字证书的流程的如下：

1、持有人将公钥以及身份信息发送给权威机构。

2、权威机构负责对持有人的身份进行验证，确保公钥和持有人的信息准确无误。

3、权威机构使用自己私钥对持有人公钥进行数字签名，生成数字证书。

4、为了确保证书不被篡改，权威机构对数字证书进行hash计算（指纹算法），生成摘要（指纹），使用自己的私钥对摘要进行数字签名，放到数字证书中。

5、对持有人收费。

附：

几篇好的文章，对我的帮助很大，谢谢作者：

http://www.ruanyifeng.com/blog/2011/08/what_is_a_digital_signature.html

http://blog.csdn.net/ly131420/article/details/38400583

分类: 杂项

hthf
关注 - 0
粉丝 - 2
+加关注

4 0

« 上一篇：rhel5.4 x64安装apache http server2.2.27，并创建自动启服务
» 下一篇：平安陆金所-点金计划，简直是骗子行为。

posted on 2015-11-22 19:19 hthf 阅读(11557) 评论(0) 编辑 收藏

刷新评论 刷新页面 返回顶部

注册用户登录后才能发表评论，请 登录 或 注册，访问网站首页。

相关博文：
· 数字证书
· 数字签名与数字证书
· 轻松理解数字签名和数字证书的关系
· 数字签名与数字证书
· 数字签名与数字证书

最新新闻：
· 潜望 | 马斯克的脑机接口距离我们还有多远?
· 第3个神秘快速射电暴：来源距离地球79亿光年大型星系
· 华为拍月亮方法已申请专利：拍高清月亮就看它了
· SpaceX发动机测试出小意外：星际飞船原型变"火球"
· 个人破产制度有望试点，这意味着什么?
» 更多新闻...