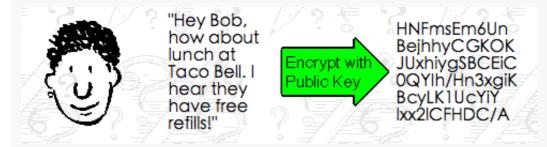


鲍勃有两把钥匙,一把是公钥,另一把是私钥。





鲍勃把公钥送给他的朋友们----帕蒂、道格、苏珊----每人一把。



苏珊要给鲍勃写一封保密的信。她写完后用鲍勃的公钥加密,就可以达到保密的效果。



HNFmsEm6Un BejhhyCGKOK JUxhiygSBCEiC 0QYlh/Hn3xgiK BcyLK1UcYiY lxx2lCFHDC/A

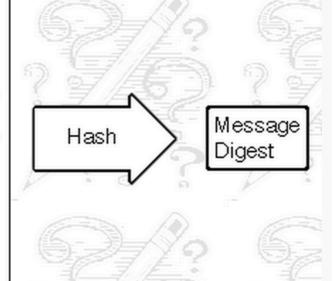


"Hey Bob, how about lunch at Taco Bell. I hear they have free refills!"

鲍勃收信后,用私钥解密,就看到了信件内容。这里要强调的是,只要鲍勃的私钥不泄露,这 封信就是安全的,即使落在别人手里,也无法解密。

The the creates of TGO Greety Good Proving, a publishing encopyring activate parking for the protection of electronic stati. Since TGO was published Goodsefacily as fromware in June of 1993, if has agreed organically all over the world, and has since became the 6th first worldwise throughout or copyright of 8 mails making assuments including whether the organization in the 18th authority awards of a mail state in week green by the 100 Customs Secretar, who the required that have some broken when TGO speed outside the US. That is variagation was closed without indictant tim January 1995.

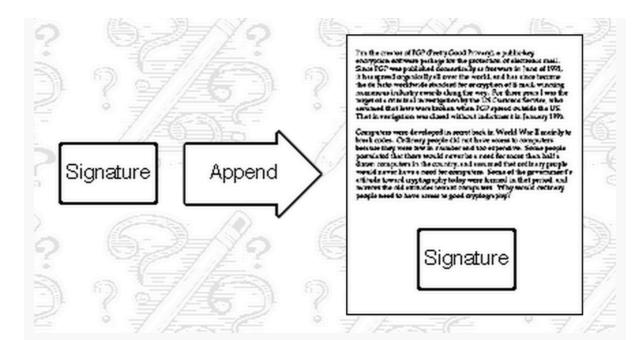
Consystem were developed in secret took in World Wie Enterinly below to close. Colleany people (d) not there were to computers because they more new in reamber and too expective. Some people portained that there would never be a need for more than half's distort computers in the country, and same not test collinary people would never have a need for enterpaires. Some of the preventment of either to more durying puly today were formed in their provide and increase the old entering entered contract computers. Why securil contrary people need to have a research good cryptography?



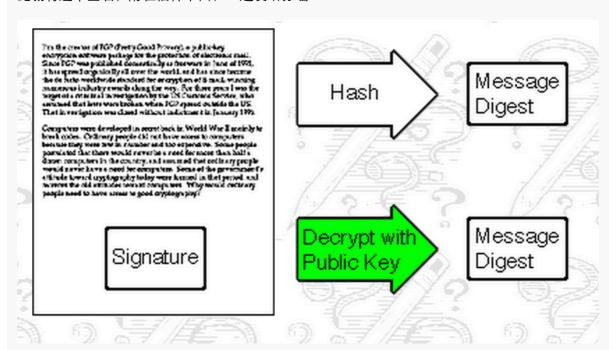
鲍勃给苏珊回信,决定采用"数字签名"。他写完后先用Hash函数,生成信件的摘要(digest)。



然后,鲍勃使用私钥,对这个摘要加密,生成"数字签名"(signature)。

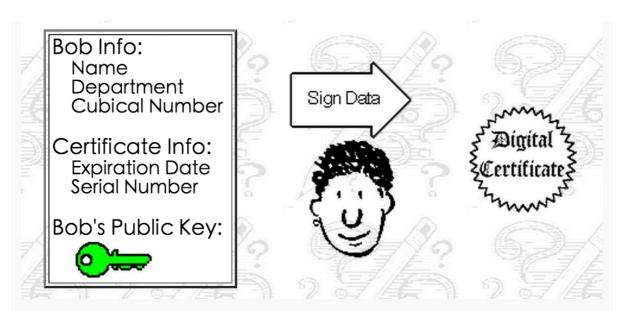


鲍勃将这个签名,附在信件下面,一起发给苏珊。



苏珊收信后,取下数字签名,用鲍勃的公钥解密,得到信件的摘要。由此证明,这封信确实是鲍勃发出的。 苏珊再对信件本身使用Hash函数,将得到的结果,与上一步得到的摘要进行对比。如果两者一致,就证明这封信未被修改过。

复杂的情况出现了。道格想欺骗苏珊,他偷偷使用了苏珊的电脑,用自己的公钥换走了鲍勃的公钥。此时,苏珊实际拥有的是道格的公钥,但是还以为这是鲍勃的公钥。因此,道格就可以冒充鲍勃,用自己的私钥做成"数字签名",写信给苏珊,让苏珊用假的鲍勃公钥进行解密。



后来,苏珊感觉不对劲,发现自己无法确定公钥是否真的属于鲍勃。她想到了一个办法,要求鲍勃去找"证书中心"(certificate authority,简称CA),为公钥做认证。证书中心用自己的私钥,对鲍勃的公钥和一些相关信息一起加密,生成"数字证书"(Digital Certificate)。

鲍勃拿到数字证书以后,就可以放心了。以后再给苏珊写信,只要在签名的同时,再附上数字证书就行了。

苏珊收到Bob的信,先用CA的公钥解开数字证书,就可以拿到鲍勃真实的公钥了,然后就能证明"数字签名"是否真的是鲍勃签的。