2002年图灵奖
公钥密码学
RSA加密算法

刘正 徐小奇

December 3, 2013

加密的历史

1976年以前，所有的加密方法都是同一种模式：

加密的历史

1976年以前，所有的加密方法都是同一种模式：

- 甲方选择某一种加密规则，对信息进行加密；

加密的历史

1976年以前，所有的加密方法都是同一种模式：

- 甲方选择某一种加密规则，对信息进行加密；
- 乙方使用同一种规则，对信息进行解密。

加密的历史

1976年以前，所有的加密方法都是同一种模式：

- 甲方选择某一种加密规则，对信息进行加密；
- 乙方使用同一种规则，对信息进行解密。

由于加密和解密使用同样规则（简称”密钥”），这被称为”对称加密算法”（Symmetric-key algorithm）。

这种加密模式有一个最大弱点：甲方必须把加密规则告诉乙方，否则无法解密。保存和传递密钥，就成了最头疼的问题。

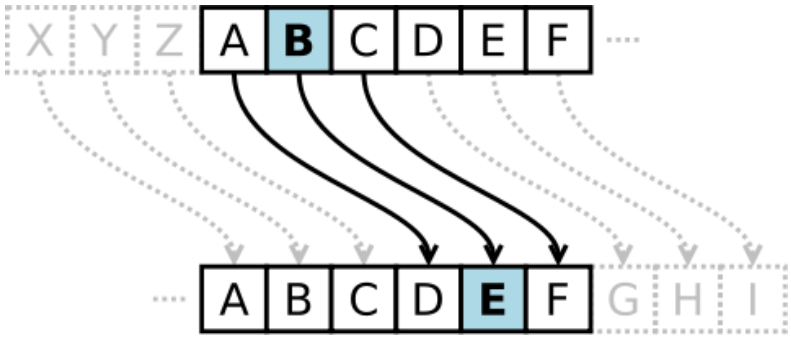
凯撒密码

凯撒密码

字母之间的替换—它的几个变种：换字式密码(破解的方法可以使用字符频数分析法)、转置式密码、多表替换密码(先分组后凯撒加密)

凯撒密码

字母之间的替换—它的几个变种：换字式密码(破解的方法可以使用字符频数分析法)、转置式密码、多表替换密码(先分组后凯撒加密)



栅栏密码

栅栏密码

所谓栅栏密码，就是把要加密的明文分成N个一组，然后把每组的第1个字连起来，形成一段无规律的话。 不过栅栏密码本身有一个潜规则，就是组成栅栏的字母一般不会太多。（一般不超过30个，也就是一、两句话）

RSA加密算法

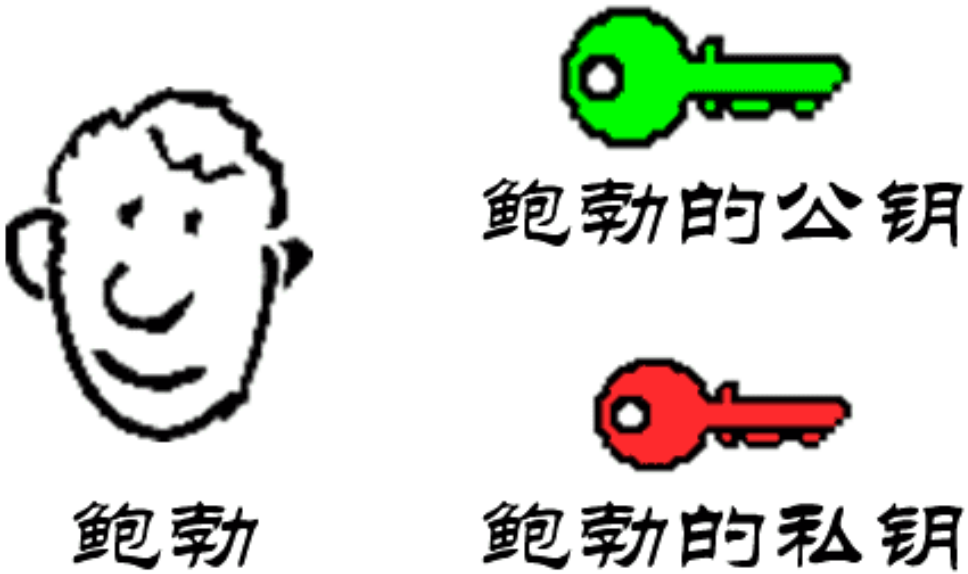
RSA加密算法

RSA加密算法是一种非对称加密算法。在公开密钥加密和电子商业中RSA被广泛使用。

RSA是1977年由罗纳德·李维斯特（Ron Rivest）、阿迪·萨莫尔（Adi Shamir）和伦纳德·阿德曼（Leonard Adleman）一起提出的。当时他们三人都在麻省理工学院工作。RSA就是他们三人姓氏开头字母拼在一起组成的。

1973年，在英国政府通讯总部工作的数学家克利福德·柯克斯（Clifford Cocks）在一个内部文件中提出了一个相同的算法，但他的发现被列入机密，一直到1997年才被发表。

RSA加密算法



鲍勃有两把钥匙，一把是公钥，另一把是私钥。

RSA加密算法

鲍勃把公钥送给他的朋友们——帕蒂、道格、苏珊——每人一把。

RSA加密算法

苏珊

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

公钥加密

HNFmsEm6Un
BejhhyCGKO
KJUxhiygSBC
EiC0QYIh/Hn
3xgiKBcyLK1
UcYiYlxx2lCF
HDC/A

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。

RSA加密算法

HNFmsEm6Un
BejhhyCGKO
KJUxhiygSBC
EiC0QYIh/Hn
3xgiKBcyLK1
UcYiYlxx2lCF
HDC/A

私钥解密

"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。

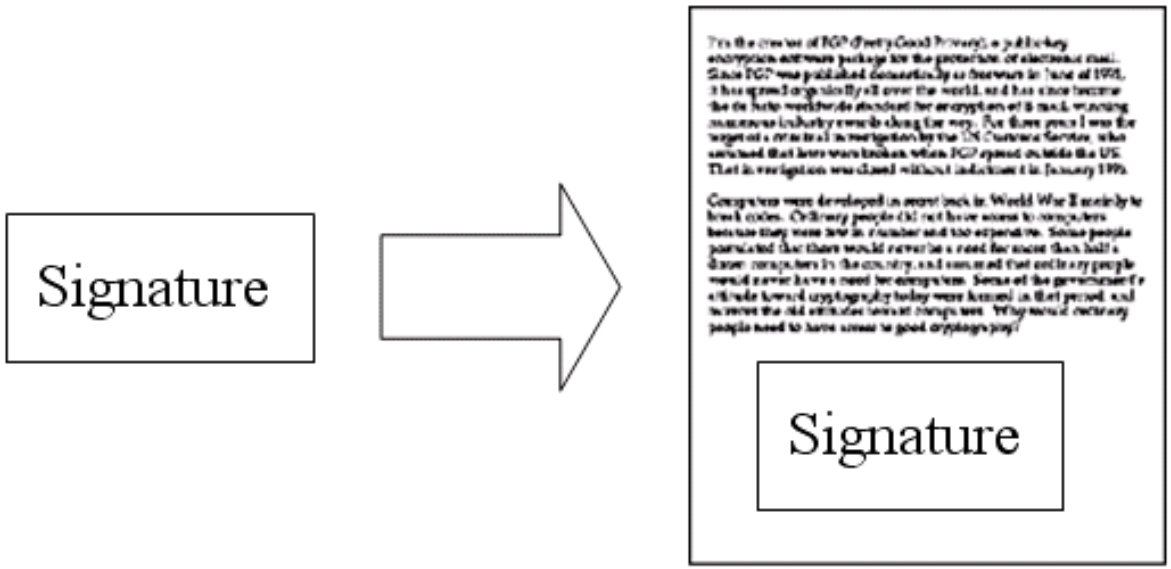
RSA加密算法

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）。

RSA加密算法

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

RSA加密算法

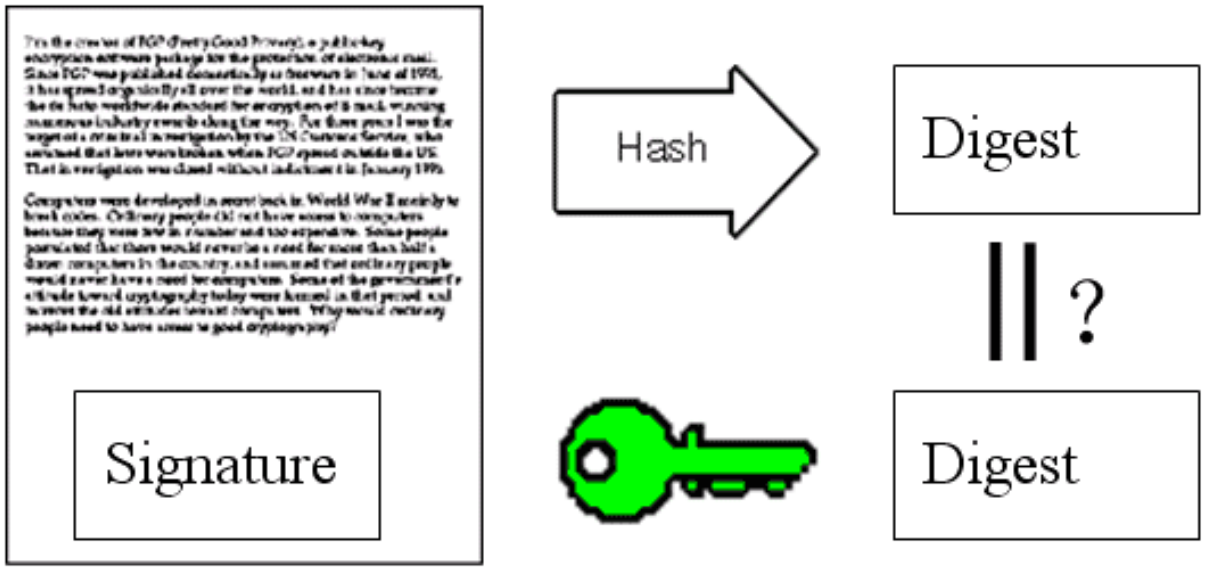


鲍勃将这个签名，附在信件下面，一起发给苏珊。

RSA加密算法

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。

RSA加密算法

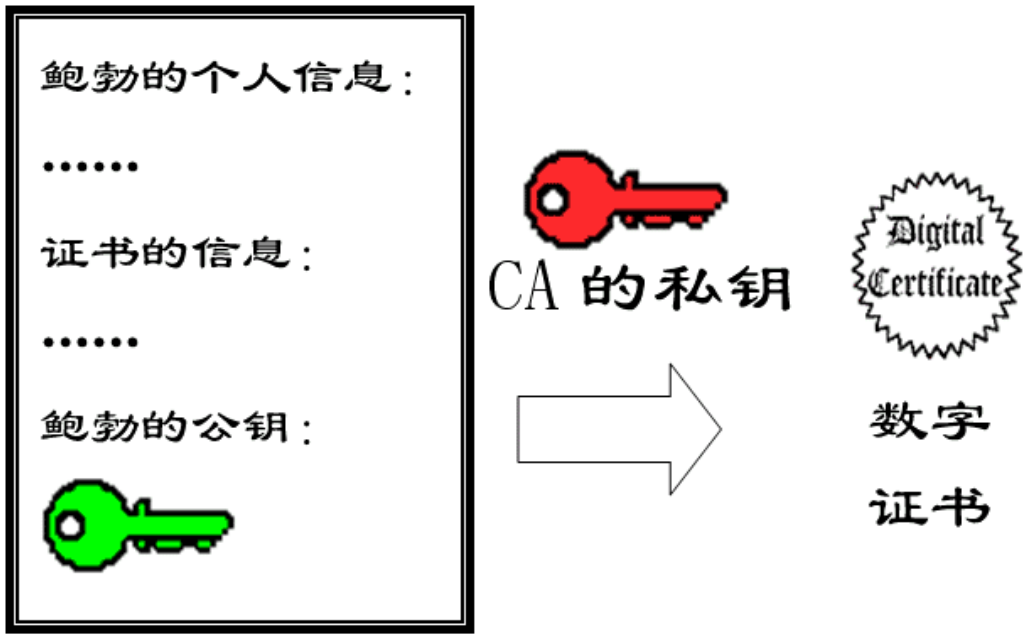


苏珊再对信件本身使用Hash函数，将得到的结果，与上一步得到的摘要进行对比。如果两者一致，就证明这封信未被修改过。

RSA加密算法

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。

RSA加密算法

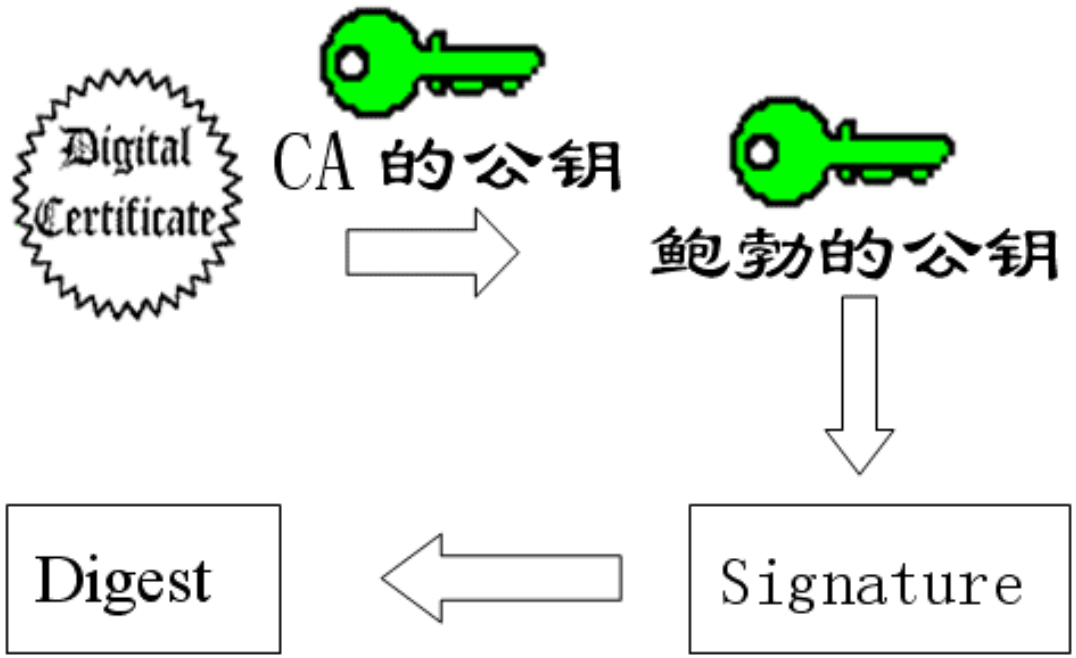


后来，苏珊感觉不对劲，发现自己无法确定公钥是否真的属于鲍勃。她想到了一个办法，要求鲍勃去找”证书中心”（certificate authority，简称CA），为公钥做认证。证书中心用自己的私钥，对鲍勃的公钥和一些相关信息一起加密，生成”数字证书”（Digital Certificate）。

RSA加密算法

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。

RSA加密算法



苏珊收信后，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。

获奖啦

获奖啦

Clifford Cocks

1950,Prestbury, Cheshire, United Kingdom

He invented the widely used encryption algorithm now commonly known as RSA, about three years before it was independently developed by Rivest, Shamir, and Adleman at MIT. He has not been generally recognised for this achievement because his work was classified information, and therefore not released to the public at the time.

Ronald L. Rivest

1947, Schenectady, New York, USA

BA (Mathematics, Yale University, 1969);

PhD (Computer Science, Standford University, 1973);

Robert W Floyd. 1978.

Donald Ervin Knuth. 1974.

Postdoctoral (Computer Science, INRIA, 1975);

RSA Algorithm 1977

RSA Data Security 1983

Introduction to Algorithms 1990

Adi Shamir

July 6, 1952, Tel Aviv, Israel

BSc (Mathematics, Tel Aviv University, 1973);

MSc (Computer Science, Weizmann Institute, Israel, 1975);

PhD (Computer Science, Weizmann Institute, Israel, 1977)

Shamir’ s Secret Sharing.

Attack DES, 1977

Identity-based crtyptography, 1984

Visual cryptography, 1994

Leonard M. Adleman

December 31, 1945, San Francisco, USA

BA, Mathematics (University of California, Berkley, 1968);

PhD, Computer Science (University of California, Berkley, 1976).

Professor (University of Southern California, 1980).

Godfather Of Computer Virus, Student Cohen. 1983.

Father of DNA Computing.

Fermat’ s Last Theorem 1986.

Hollywood Film Sneakers, mathmatical and cryptography consultant 1992

八卦环节

当年第一个公开密钥算法是背包算法，其发明者Ralph Merkle对这个算法极有信心，确信这个算法不可能被攻破，所以他悬赏100美元奖金给破解算法的人。Adi Shamir迅速破解了该算法，并领走了奖金。Shamir就是RSA算法的发明人之一。

但Merkle并没有气馁，他又加强了算法，并悬赏1000美元奖金，给破解新算法的人。结果Ronald Rivest也迅速地破解了该算法，并领走了奖金。Rivest是RSA算法的另一个发明人。

于是，Merkle终于没有胆量尝试第三次悬赏，于是RSA的最后一个作者Leonard Adleman也就没有机会成为万元户了。（按照规律，Merkle如果要悬赏，应该是10000美金了。）