2002年图灵奖 公钥密码学 RSA加密算法

刘正 徐小奇

November 27, 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。

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。

Ronald L. Rivest

Adi Shamir

Leonard M. Adleman

Clifford Cocks

我是中文

- one

刘正 徐小奇 e

我是中文

- one
- two

刘正 徐小奇 e

我是中文

- one
- two
- three

刘正 徐小奇 e

我是中文

- one
- two
- three
- four

刘正 徐小奇 e

我是中文

- one
- two
- three
- four
- five

刘正 徐小奇 e

我是中文

- one
- two
- three
- four
- five
- six

刘正 徐小奇 e