

2002年图灵奖 公钥密码学 RSA加密算法

刘正 徐小奇

RSA加密算法 获奖者生平

八卦环节

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

2002年图灵奖 公钥密码学 RSA加密算法

刘正 徐小奇

RSA加密算法

获奖者生平

八卦环节

1976年以前,所有的加密方法都是同一种模式:



2002年图灵奖 公钥密码学 RSA加密算法

刘正 徐小奇

Vatt 194.1.40

RSA加密算法

获奖者生平

八卦环节

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;



2002年图灵奖 公钥密码学 RSA加密算法

刘正 徐小奇

RSA加密算法

获奖者生平 八卦环节

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

• 乙方使用同一种规则,对信息进行解密。



2002年图灵奖 公钥密码学 RSA加密質法

刘正 徐小奇

RSA加密質法

获奖者生平

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。



2002年图灵奖 公钥密码学

刘正 徐小奇

RSA加密質法

获奖者生平

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

2002年图灵奖 公钥密码学 RSA加密算法

刘正 徐小奇

RSA加密算法

获奖者生平

八卦环节



Adi Shamir

2002年图灵奖 公钥密码学 RSA加密算法

刘正 徐小奇

RSA加密算法

获奖者生平 八卦环节



Leonard M. Adleman

2002年图灵奖 公钥密码学 RSA加密算法

刘正 徐小奇

RSA加密算法

获奖者生平

八卦环节



Clifford Cocks

2002年图灵奖 公钥密码学 RSA加密算法

刘正 徐小奇

RSA加密算法 获奖者生平

八卦环节



2002年图灵奖 公钥密码学 RSA加密算法

刘正 徐小奇

对正 体小点

RSA加密算法 获奖者生平

狄头白土节

八卦环节

刘正 徐小奇 e

one



2002年图灵奖 公钥密码学 RSA加密算法

刘正 徐小奇

RSA加密算法 获奖者生平

八卦环节

- one
- two



2002年图灵奖 公钥密码学 RSA加密算法

刘正 徐小奇

RSA加密算法 获奖者生平

八卦环节

- one
- two
- three



2002年图灵奖 公钥密码学 RSA加密算法

刘正 徐小奇

RSA加密算法

获奖者生平

八卦环节

- one
- two
- three
- four



2002年图灵奖 公钥密码学 RSA加密算法

刘正 徐小奇

RSA加密算法

获奖者生平

八卦环节

- one
- two
- three
- four
- five



2002年图灵奖 公钥密码学 RSA加密算法

刘正 徐小奇

RSA加密算法

获奖者生平

八卦环节

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