§3.5 其他分组密码算法

一、IDEA

国际数据加密算法(IDEA)与DES一样，也是一种使用一个密钥对64位数据块进行加密的单钥加密算法，它是瑞士联邦技术学院开发的一种面向数据分组块的数据加密标准。

相对于DES的56位密钥，它使用128位密钥，每次加密一个64位数据块，这么长的密钥被认为即使在多年后仍是有效的。

IDEA算法通过一系列的加密轮次进行操作，每轮都使用从完整的加密密钥中生成的一个子密钥，使用一个称为“压码”的函数在每轮中对数据位进行编码。与DES不同的是IDEA不使用置换。

§3.5 其他分组密码算法

一、IDEA

IDEA算法的安全性相对DES算法有很大的提高，其密钥是128位，在穷举攻击的情况下，需要经过2^{128}次加密才能恢复出密钥。假设一台计算机每秒产生和运行10亿个密钥，它将检测10^{13}年。

至今IDEA还没有明显的安全漏洞，就连PGP（安全电子邮件）中也采用IDEA作为数据加密。

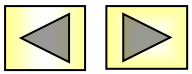
§3.5 其他分组密码算法

二、 RC5/ RC6

RC5是对称加密算法，由RSA公司的首席科学家R.Rivest于1994年设计，1995年正式公开的一个很实用的加密算法。

RC5自1995年公布以来，尽管至今为止还没有发现实际攻击的有效手段，然而一些理论攻击的文章先后也分析出RC5的一些弱点。

RC6是RC5的进一步改进，被选为21世纪加密标准算法。像RC5那样，RC6实际上是利用数据的循环移位。



§3.5 其他分组密码算法

三、 AES

NIST(国家标准技术研究所)1997年9月12日发出征集高级加密标准的通知 。1998年8月首次选出15个候选者，1999年3月选出5个，包括：E2、MARS、RC6、Rijndael、Twofish。2000年10月2日，美国商务部部长宣布比利时的Rijndael算法成为新的AES。

选择的基本条件：公开；分组单钥，分组长度128；密钥可为128，192，256；可软硬件实现。

AES被开发用于替代DES，但NIST预测三重DES仍将在近期作为一种实用的算法，单DES将逐步退出。