# <<经典密码学与现代密码学>>

## 图书基本信息

书名：<<经典密码学与现代密码学>>

13位ISBN编号：9787302107408

10位ISBN编号：7302107408

出版时间：2005-7

出版时间：清华大学出版社

作者：(美)斯皮尔曼

译者：叶阮健 曹英 张长富

# <<经典密码学与现代密码学>>

## 内容概要

《经典密码学与现代密码学》主要从三个方面来介绍密码学的知识：第一部分介绍了经典密码学的经典问题，包括单码加密法、仿射加密法、多码加密法、多图加密法和换位加密法；第二部分介绍了现代密码学，包括流加密法、块加密法和公钥加密法；第三部分介绍了密码学的未来，并对量子加密法进行了简单介绍。
《经典密码学与现代密码学》一个突出的特点足，对密码破解进行了详细描述，使读者既掌握加密的内部算法，又能了解各种加密法的弱点。
与《经典密码学与现代密码学》配套的CAP软件实现了各种加密法，读者可以利用该软件进行加密和解密，从而增强了《经典密码学与现代密码学》的科学性和适用性。
每章末尾还给出了一些复习题，给读者以很大的启发和想象力。

《经典密码学与现代密码学》不仅是一本很好的密码学教材，对密码学研究人员和广大密码学爱好者也都是一本不可多得的参考用书。

# <<经典密码学与现代密码学>>

## 书籍目录

# <<经典密码学与现代密码学>>

## 版权说明