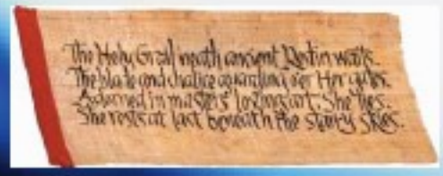
数据加密技术

教师:庄志宏

LOGO



密码学起源

- 最先有意识的使用一些技术的方法来加密信息的可能是公元六年前的古希腊人。他们使用的是一根叫scytale的棍子。送信人先绕棍子卷一张纸条，然后把要写的信息纵写在上面，接着打开纸送给收信人。如果不知道棍子的宽度（这里作为密匙）是不可能解密里面的内容的。后来，罗马的军队用凯撒密码（三个字母表轮换）进行通信。

- 在随后的19个世纪里面，主要是发明一些更加高明的加密技术，这些技术的安全性通常依赖于用户赋予它们多大的信任程度。在19世纪Kerchoffs写下了现代密码学的原理。其中一个的原理提到：加密体系的安全性并不依赖于加密的方法本身，而是依赖于所使用的密匙。

- 密码信很简单，很容易被破解，基本上制作密码信和使用电子密码方案一样由一个明文，加密算法，到密码的过程。由于简单易破，现在很少使用原始的密码信了。

Ⅰ. 密码学基础

引言

(1)数据加密

(2)密文与加密算法强度的关系

引言

- 2006年的电影《达·芬奇密码》相信大家都应该印象深刻

引言

- 里面主要围绕着解密过程来展开剧情，而加密解密这事实上在我们生活的各个领域都存在着只是大家没有注意到。

引言

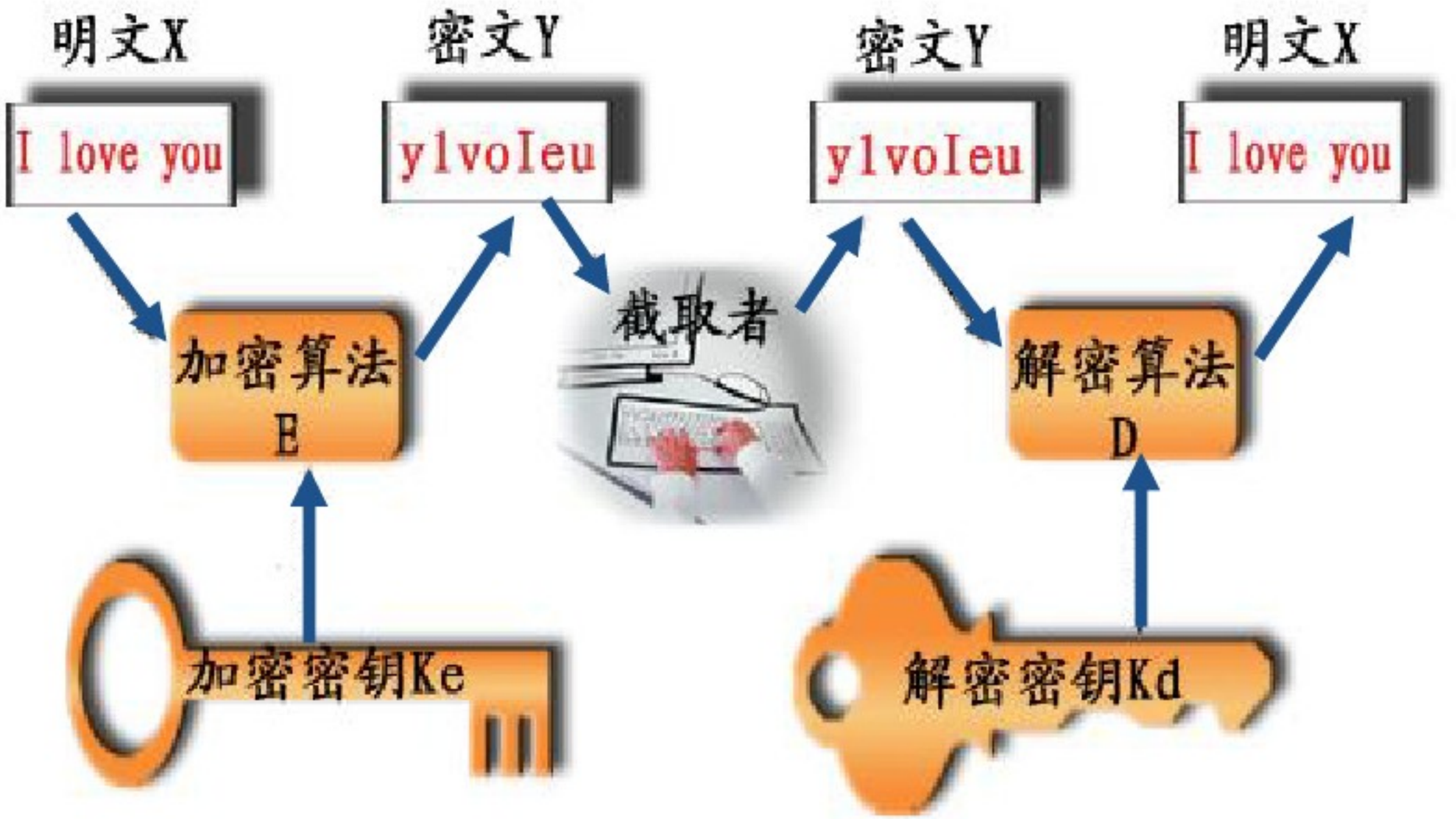
- 那现在让我们来了解下商务当中存在的密码应用。

(1)数据加密

- 数据加密就是将密码学应用在数据传递过程中，保证数据的安全性，其中：利用密码技术可以把某些重要信息或数据从一个可理解的明文形式变换成为一种错乱的、不可理解的密文形式，称为**加密过程**；密文经过线路传送到达目的端后，用户按特定的解密方法将密文还原为明文，称为**解密的过程**。

(1)数据加密

- 下图就是一个很典型的加密码过程图：



⑵密文与加密算法强度的关系

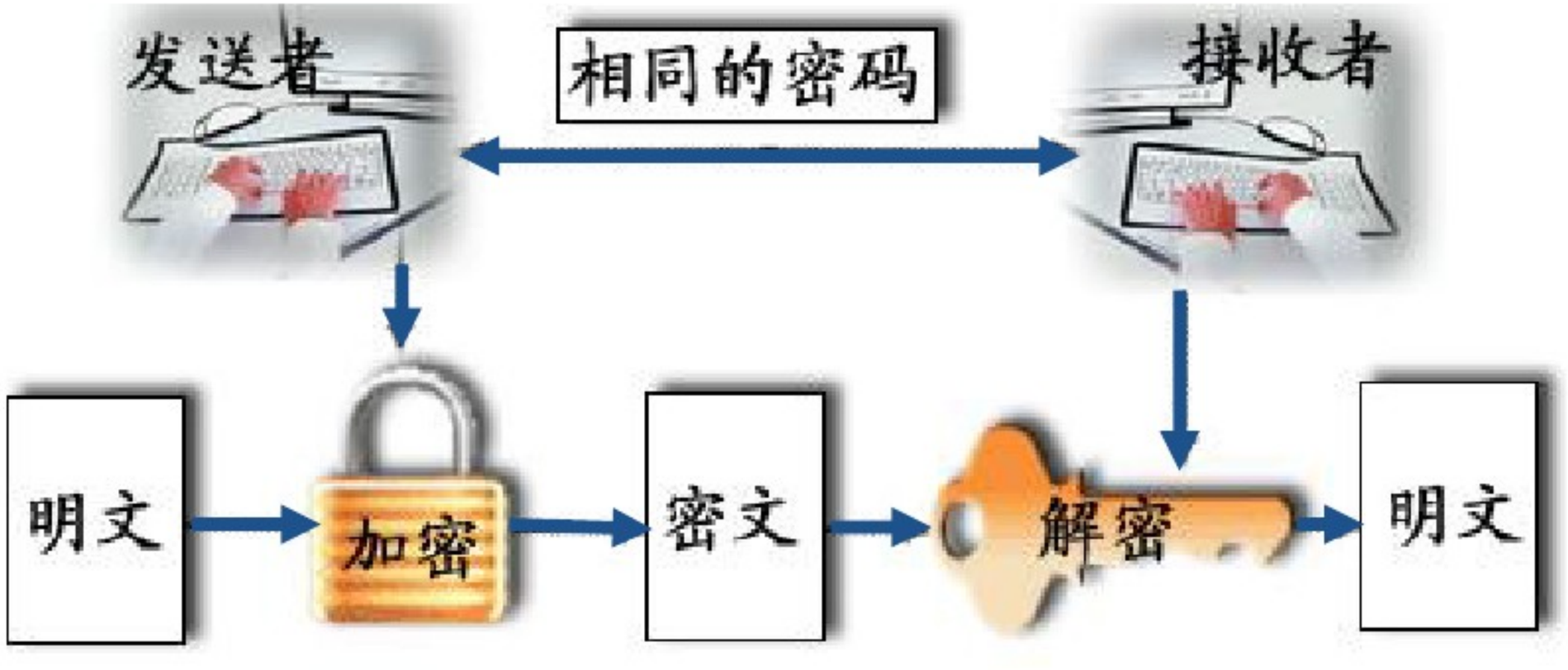
- 一种密文的保密程度与加密算法的强度（或称算法杂度）相关，加密强度越大，密文越不容易被破译，保密性也就越好；然而，随着加密强度的加大，算法的计算复杂亦会相应增加，加密解密的执行效率也会相应降低。因此，全理确定系统的加密强度也是一个成功电子交易系统的一个重要环节。
- 密码技术是最常用的安全交易手段，在电子商务中常用的加密方法有传统密钥密码方法和公开密钥密码方法两类。前者以数据加密标准DES算法为典型代表，后者通常以RSA算法为代表。

Ⅱ. 对称密钥加密与数据加密标准（DES）

- (1)密钥特点
- (2)DES算法
- (3)优缺点
- (4)应用普及

(1)密钥特点

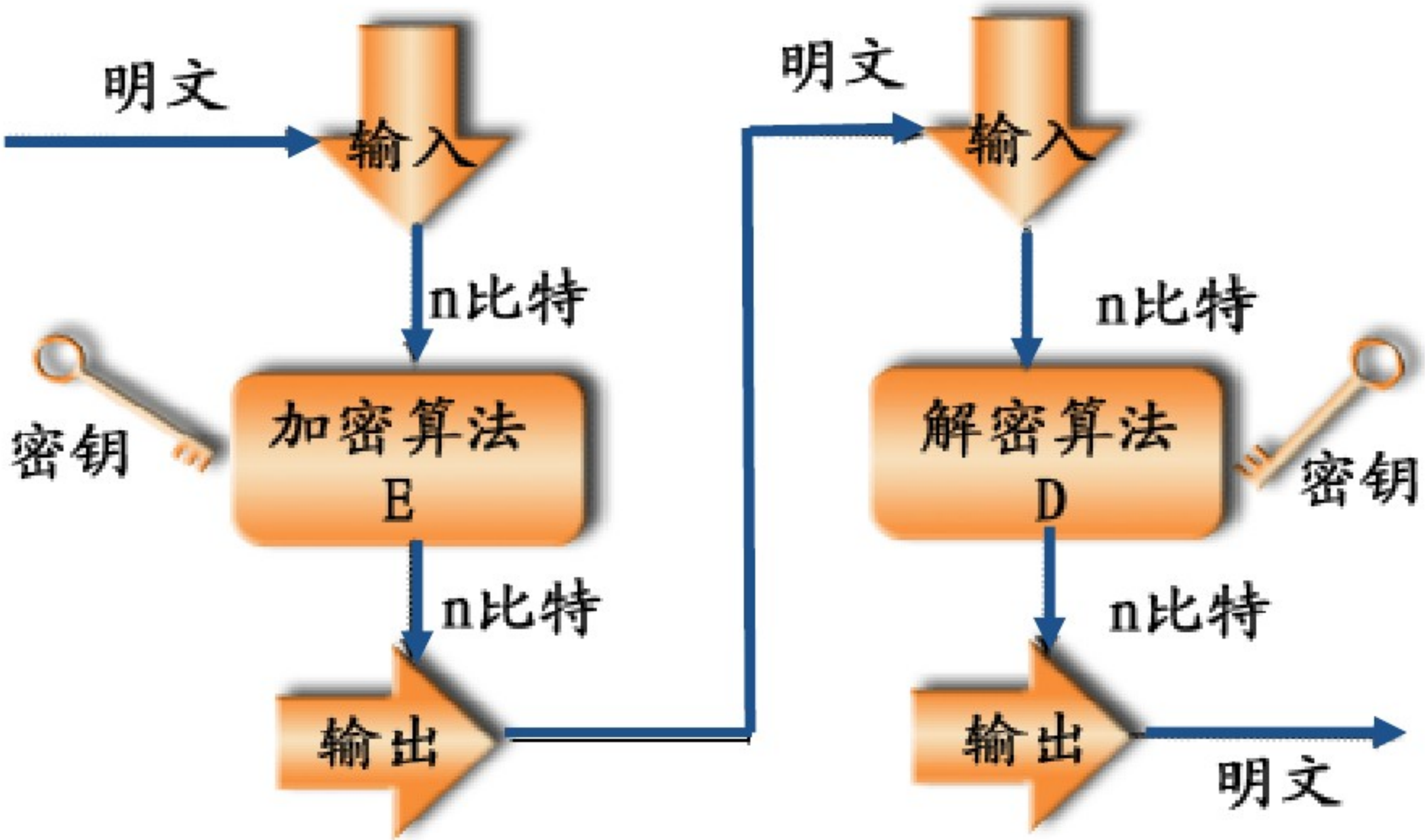
- 对称密钥加密算法是指文件加密和解密使用一个相同秘密密钥，也叫会话密钥。目前世界上较为通用的对称加密算法为DES。



(2)DES算法

- 数据加密标准DES算法由美国IBM公司于1972年研制成功，1979年美国银行协会批准使用DES，1980年它又成为美国标准化协会（ANSI）的标准。DES算法的基本思想来自于分组密码，即将明文划分成固定的n比特的数据组，然后以组为单位，在密钥的控制下进行一系列的线性或非线性的变化变换而得到密文，这就是分组密码（block cipher）体制。

(2)DES算法



(3)优缺点

- DES算法的优点是加密、解密速度快，算法容易实现，安全性好，迄今为止尚未找到一种在理论上破译DES的行之有效的方法；
- DES算法的缺点是密钥量短，容易被穷尽，在复杂网络中难于实现密钥管理。

小知识

穷举法与DES算法

- 穷举法又称为强力法、完全试凑法，这是对截获的密文依次用各种可能的密钥破译，对所有可能的明文加密直到与截获的密文一致为止。穷举法用时间上的牺牲换来了解的全面性保证，尤其是随着计算机运算速度的飞速发展，穷举法的形象已经不再是最低等和原始的无奈之举，比如经常有黑客在几乎没有任何已知信息的情况下利用穷举法来破译密码，足见这种方法还是有其适用的领域的
- DES算法具有极高安全性，到目前为止，除了用穷举搜索法对DES算法进行攻击外，还没有发现更有效的办法。对于56位长的密钥，如果一台计算机的速度是每一秒种检测一百万个密钥，则它搜索完全部密钥就需要将近2285年的时间，可见，这是难以实现的，当然，随着科学技术的发展，当出现超高速计算机后，我们可考虑把DES密钥的长度再增长一些，以此来达到更高的保密程度。

(4)应用普及

- 美国国家标准局1973年开始研究除国防部外的其它部门的计算机系统的数据加密标准，于1973年5月15日和1974年8月27日先后两次向公众发出了征求加密算法的公告。加密算法要达到的目的（通常称为DES 密码算法要求）主要为以下四点：
- （1）提供高质量的数据保护，防止数据未经授权的泄露和未被察觉的修改；
- （2）具有相当高的复杂性，使得破译的开销超过可能获得的利益，同时又要便于理解和掌握；
- （3）DES密码体制的安全性应该不依赖于算法的保密，其安全性仅以加密密钥的保密为基础；
- （4）实现经济，运行有效，并且适用于多种完全不同的应用。

(4)应用普及

- 1977年1月，美国政府颁布：采纳IBM公司设计的方案作为非机密数据的正式数据加密标准（DES Data Encryption Standard）。
- 目前在国内，随着三金工程尤其是金卡工程的启动，DES算法在POS、ATM、磁卡及智能卡（IC卡）、加油站、高速公路收费站等领域被广泛应用，以此来实现关键数据的保密，如信用卡持卡人的PIN的加密传输，IC卡与POS间的双向认证、金融交易数据包的MAC校验等，均用到DES算法。

小　结

- Ⅰ.密码学基础
- (1)数据加密
- (2)密文与加密算法强度的关系
- Ⅱ.对称密钥加密与数据加密标准（DES）
- (1)密钥特点
- (2)DES算法
- (3)优缺点
- (4)应用普及

作　业

- 练习册P65-第1大题:
- DES算法流程图填空

谢 谢 观 赏！

LOGO