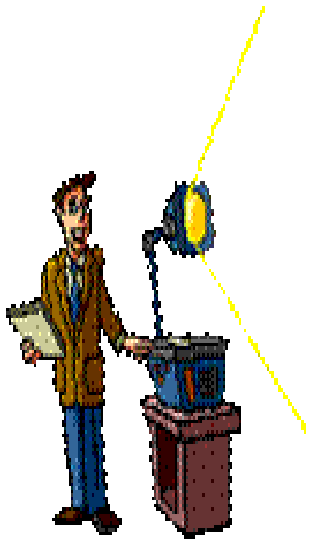
项目三 电子商务安全环境

子模块2 数据加解密技术（2学时）

内容提要：

- 电子商务安全的要求
- 数据加密技术
  - 对称密码加密体制
    - 凯撒密码
    - 多表式密码
    - DES算法



问题导入

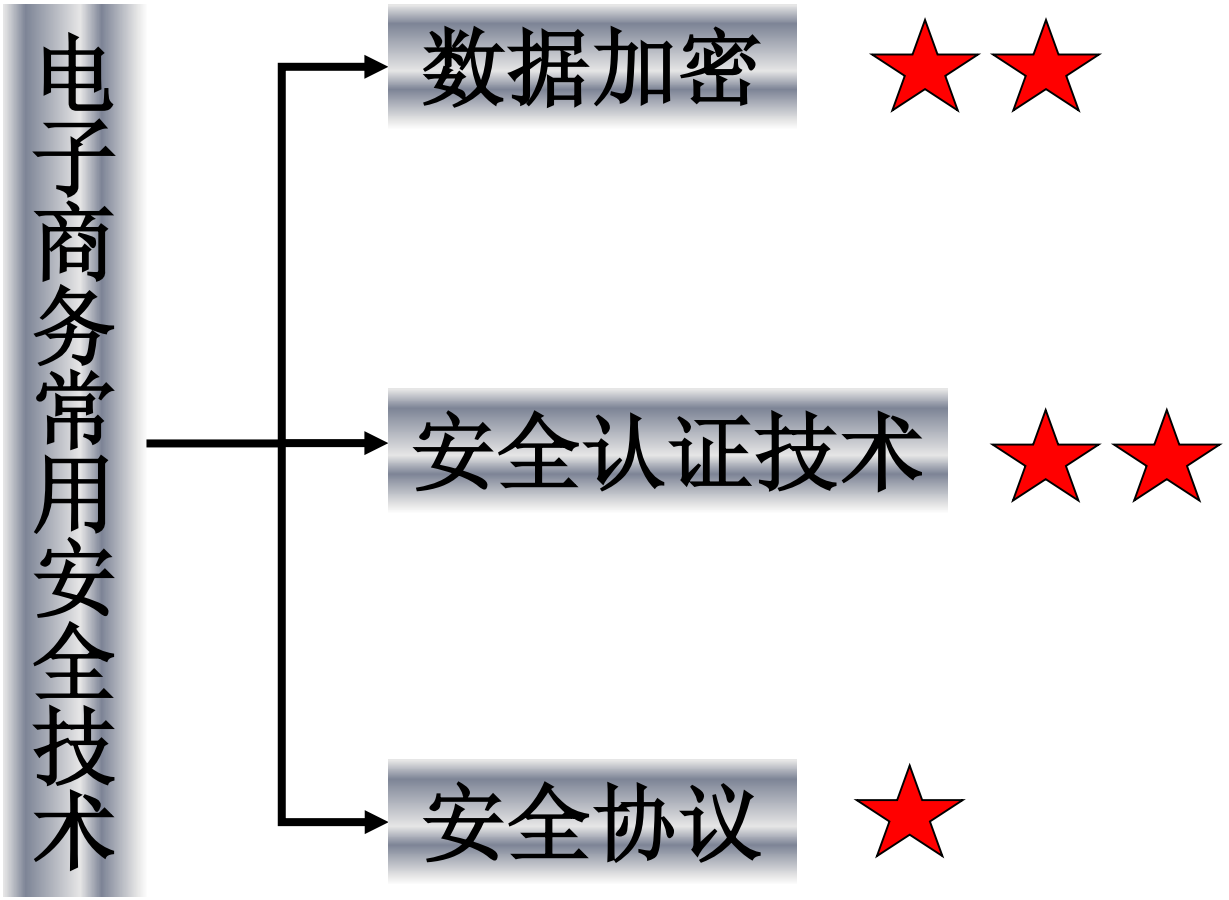
请思考电子商务交易存在哪些安全问题？

- 卖方面临问题
- 买方面临问题
- 信息传输问题
- 信用问题

电子商务安全目标

电子商务安全的基本技术要求

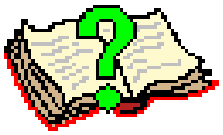
- ✓ 保密性（防止被窃取）
- ✓ 完整性（报文完整及防止被篡改）
- ✓ 不可否认性（不可抵赖性）
- ✓ 认证性（身份真实性）


电子商务常用安全技术
数据加密
安全认证技术
安全协议

数据加解密相关概念

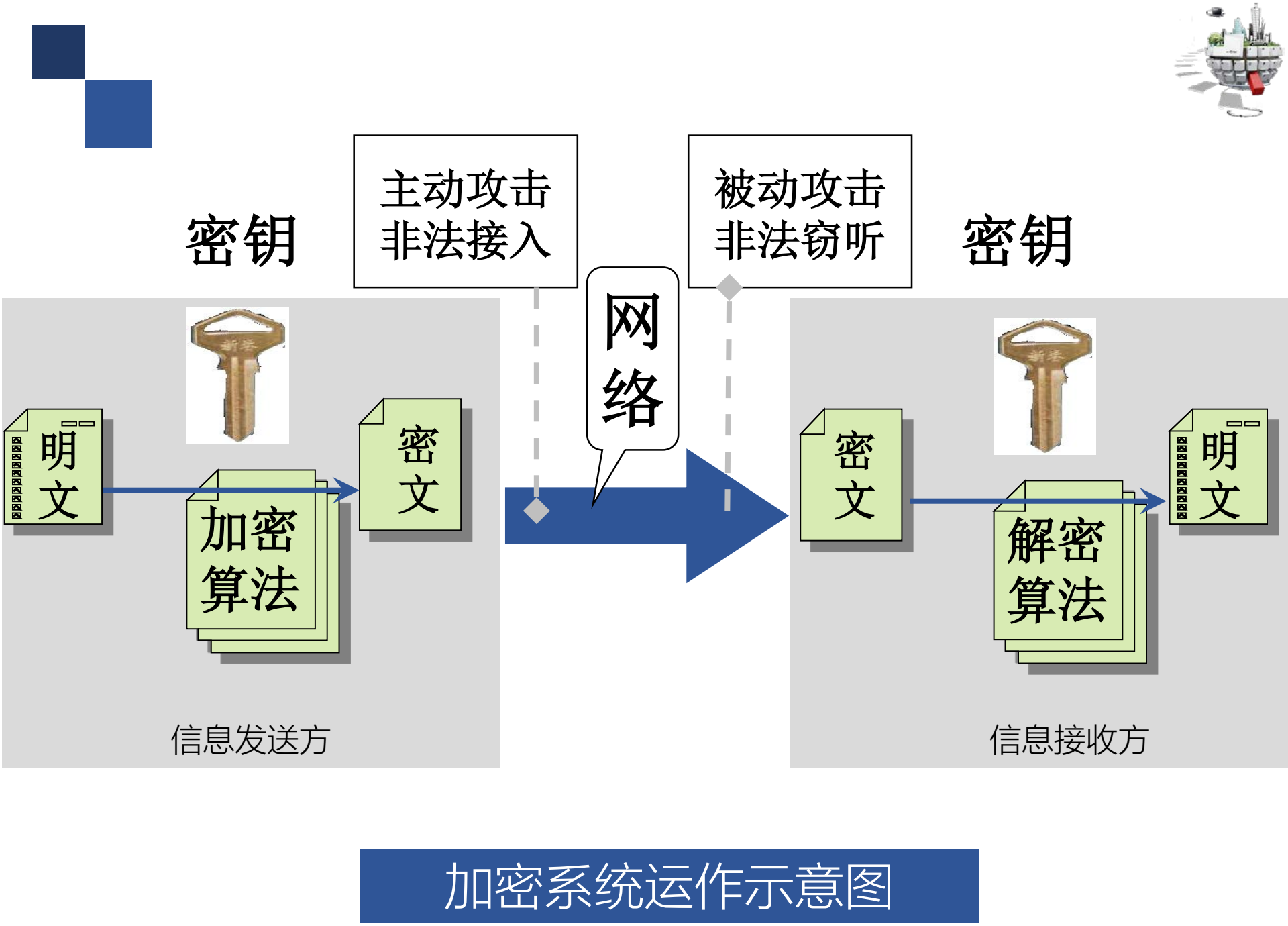
明文：被隐蔽的信息的原来可读的形式

密文：密码将明文变换成另一种隐蔽的不可理解的形式

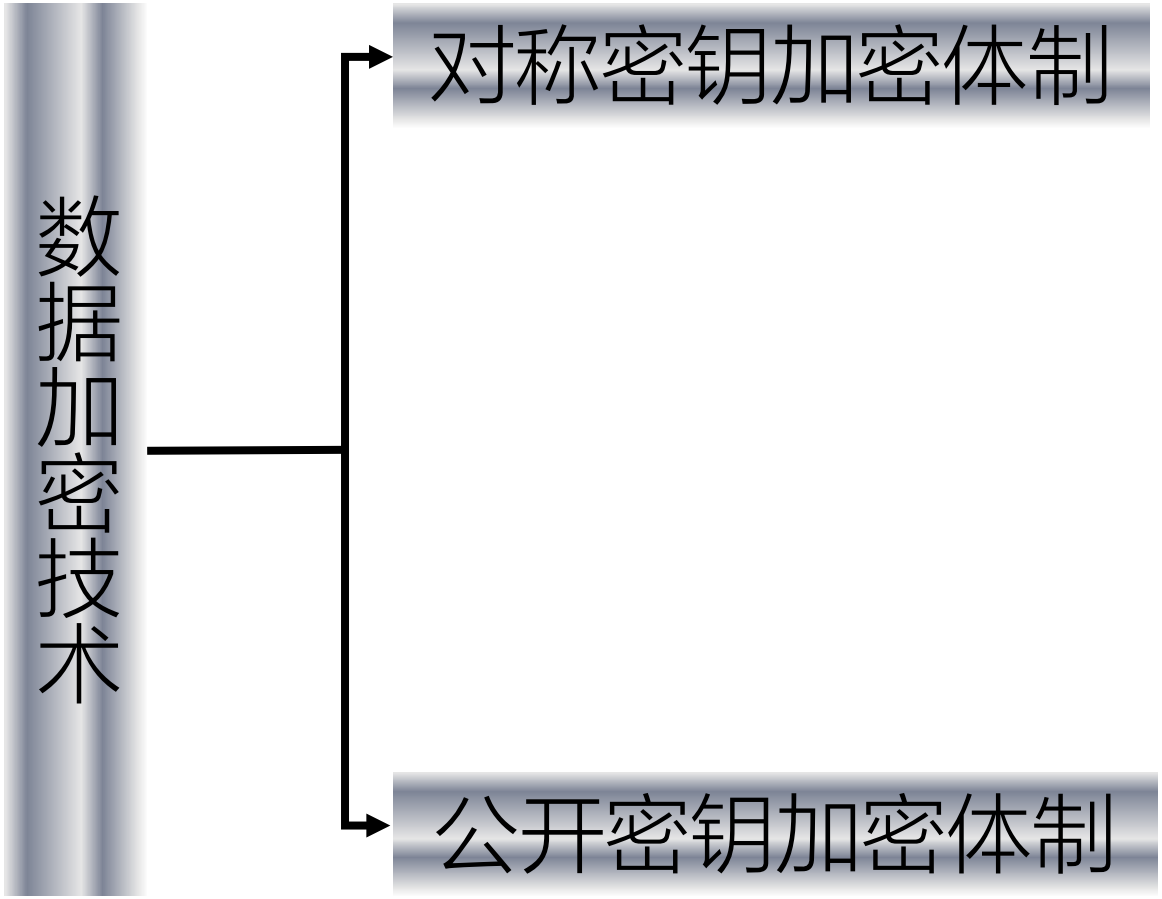


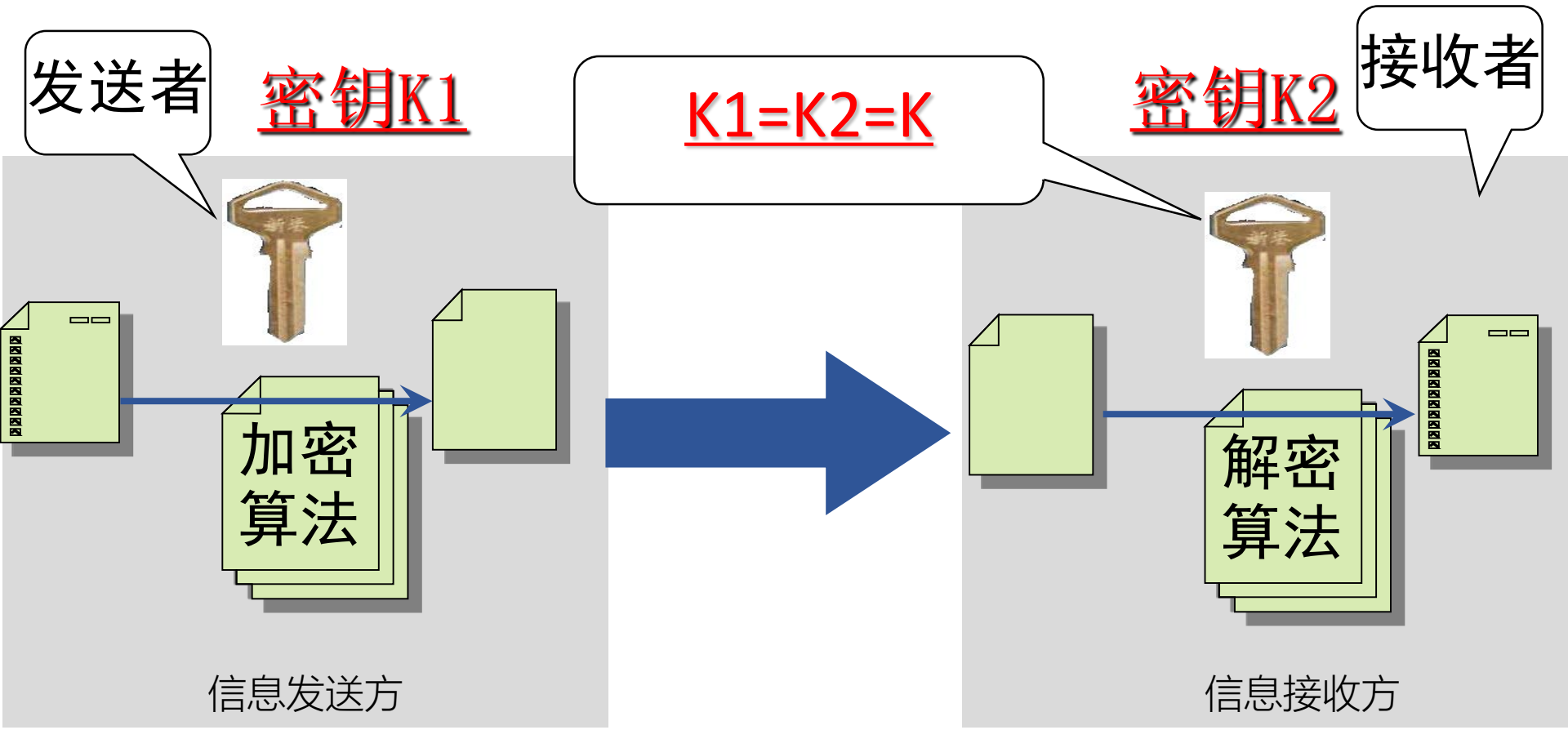
加密和解密的规则(过程）称为 **加密算法**

这一过程中辅助的一串数字或字符称为 **密钥**

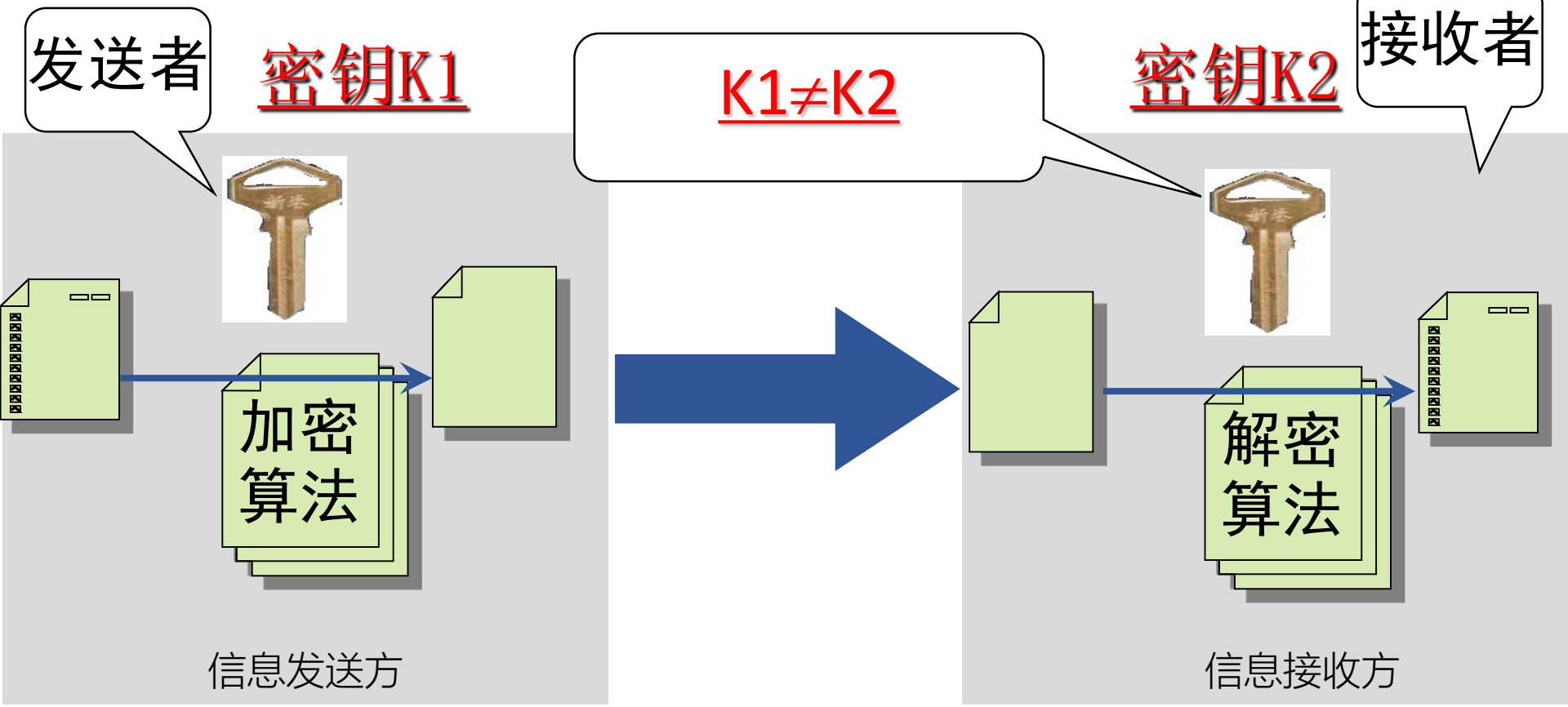


加密系统运作示意图


数据加密技术
对称密钥加密体制
公开密钥加密体制



①对称密码加密体制



②公开/非对称密码加密体制

对称密码加密体制——凯撒密码法

加密编码表示例：

字母	A	B	C	…	Z	空格
明文	01	02	03	…	26	27
密文	18	19	20	…	43	44

假设密钥=17

原文	T	h	i	s		i	s		a		s	e	c	r	e	t
明文：	20	08	09	19	27	09	19	27	01	27	19	05	03	18	05	20
密文：	37	25	26	36	44	26	36	44	18	44	36	22	20	35	22	37

凯撒密码法的破译（1）

✓ 穷举——针对密钥少

假设现已知密文，如下：

密文：PHHW PH DIWHU WKH WRJD SDUWB

密钥=1时：oggv og chvgt vjg vqic rctva

密钥=2时：mffu nf bgufs uif uphb qbsuz

密钥=3时：meet me after the toga party

.....

密钥=25时：qiix qi ejxiv xli xske tevxc

明文：meet me after the toga party

密钥为3

凯撒密码破译（2）

✓ 字母频率——针对已知明文所使用的语言

如已知密文如下所示：

UZQSOVROHXMOPVGPOZPEVSGZWSZOPFPESXUDB
METSXAIZVUEPHZHMDZSHZOWSFPAPPDTSVPQUZ
WYMXUZUHSXEPYEPOPDZSZUFPOMBZWPFUPZHM
DJUDTMOHMQ

字母P有多少个？总字母有多少个？字母P的相对频率（百分比）是多少？

凯撒密码破译（2）

密文中字母的相对频率

P	13.33	H	5.83	F	3.33	B	1.67	C	0.00
Z	11.67	D	5.00	W	3.33	G	1.67	K	0.00
S	8.33	E	5.00	Q	2.50	Y	1.67	L	0.00
U	8.33	V	4.17	T	2.50	I	0.83	N	0.00
O	7.50	X	4.17	A	1.67	J	0.83	R	0.00
M	6.67								

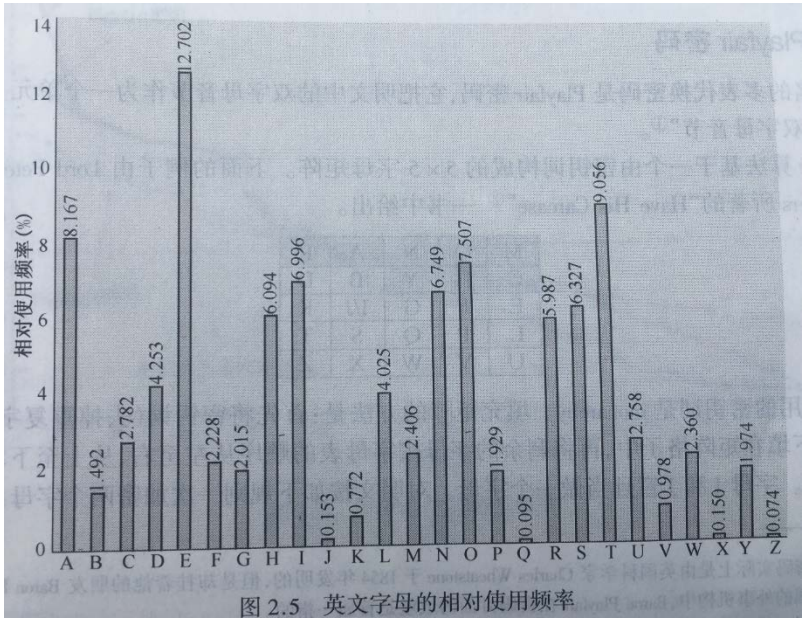


图 2.5 英文字母的相对使用频率

逐一对照比较，并结合穷举法猜测

对称密码加密体制——多表式密码法

字母	A	B	C	…	Z	空格
明文	01	02	03	…	26	27

假设密钥为“deceptive”

原文 T h i s　　i s　　a　　s e c r e t

密钥 d e c p t i v e　　d e c e p t i v

密文：xmlhtrde……

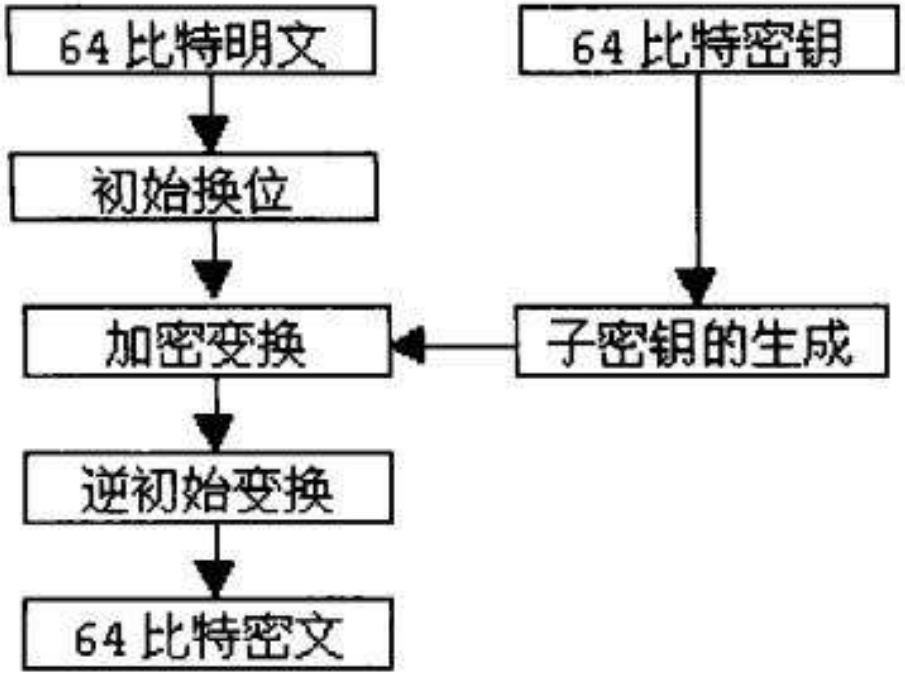
对称密码加密体制—— DES算法

如何才能隐藏明文，同时尽量减少通过“字母频率”破译的可能？

多次“代换”+“置换”、转轮机

DES算法

对称密码加密体制—— DES算法加密流程



对称密码加密体制实训

实训目的：通过CrypTool软件的应用，进一步理解对称密码加密体制的原理、特征及流程。

实训内容：

（1）使用ecxel实现凯撒加解密

（2）安装CrypTool软件

（3）实施凯撒密码法

（4）实施多表式密码

（5）实施DES算法

课程结束