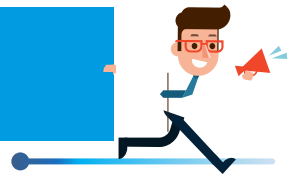
大学生计算与信息化素养

数据加密技术

本次课程所讲内容

- 数据加密技术的概念
- 密码系统

数据加密技术

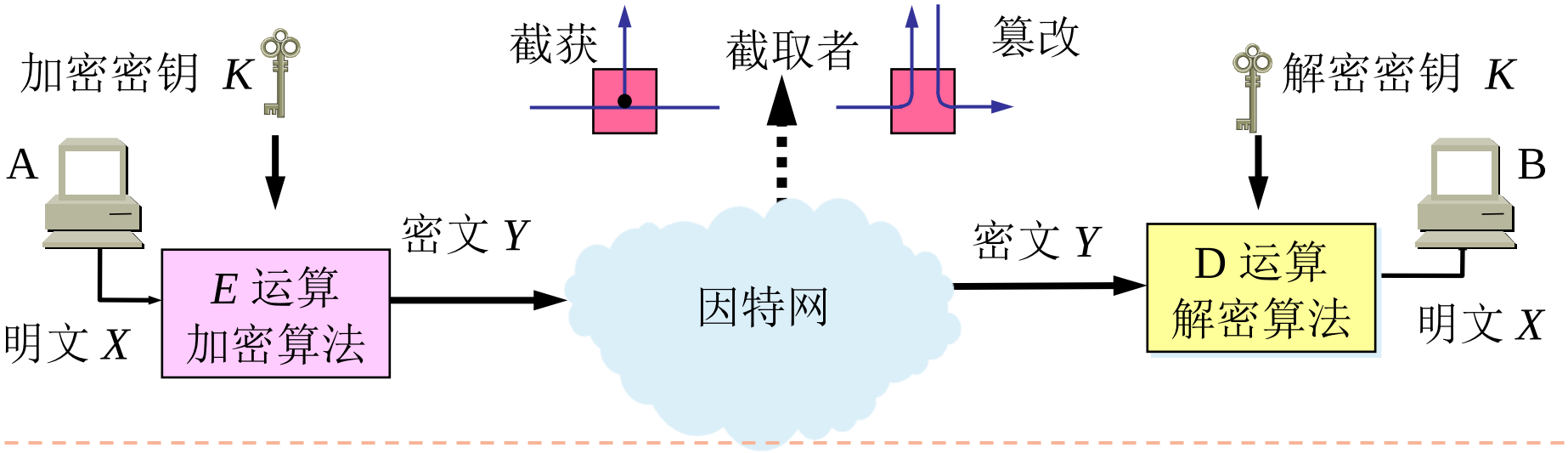


数据加密技术是指将一个信息(或称明文）经过加密密钥及加密函数转换，变成没有任何规律的密文，而接收方则将此密文经过解密函数、解密密钥还原成明文。

加密技术是网络安全技术的基石，密码学是数据加密和解密的技术基础。

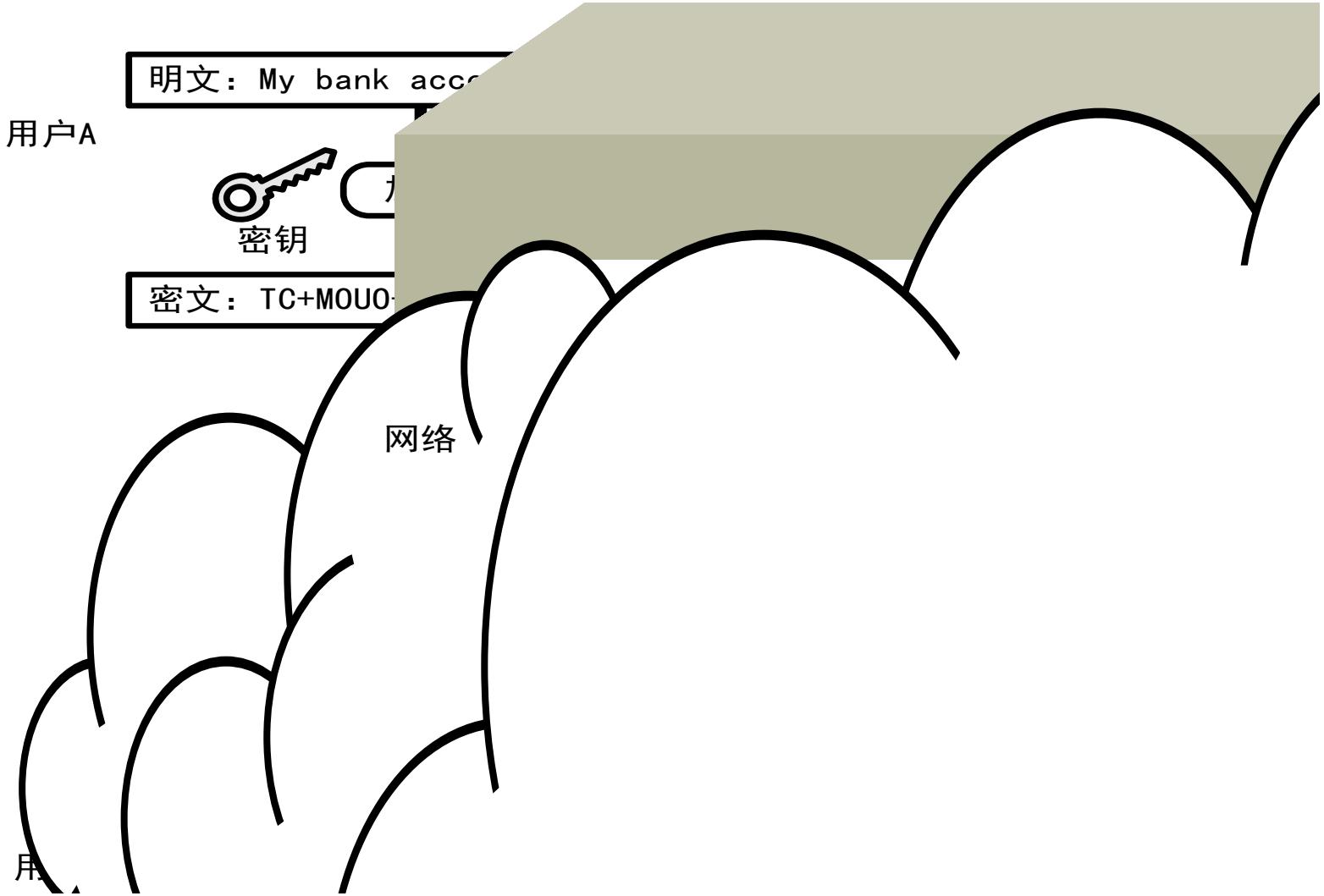
密码学分为密码编码学和密码分析学。密码编码学是对信息进行编码，实现隐蔽信息。密码分析学是是对密码进行研究分析和破译。

加密与解密过程



密码体制也叫密码系统，是指能完整地解决信息安全中的机密性、数据完整性、认证及身份识别、可控性及不可抵赖性等问题的。

加密与解密实例



密码体制

传统密码体制里所用的加密密钥和解密密钥相同，称为对称密码体制；

如果加密密钥和解密密钥不相同，则称为非对称密码体制。

密码体制有两个基本构成要素，即加密/解密算法和密钥；

在设计加密系统时，加密/解密算法是可以公开的，真正需要保密的是密钥。

我们先介绍在常规密钥密码体制（对称密钥系统）中的两种最基本的密码。

替代密码与置换密码

替代密码(substitution cipher)的原理可用一个例子来说明。（密钥是 3）

明文	abcdefghijklmnopqrstuvwxyz
密文	DEFGHIJKLMNOPQRSTUVWXYZABC

caesar cipher → FDHVDU FLSKHU

明文 c 变成了密文 F

替代密码与置换密码

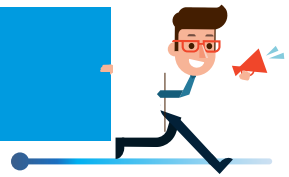
替代密码(substitution cipher)的原理可用一个例子来说明。（密钥是 3）

明文	abcdefghijklmnopqrstuvwxyz
密文	DEFGHIJKLMNOPQRSTUVWXYZABC

caesar cipher → FDHVDU FLSKHU

明文 a 变成了密文 D

替代密码与置换密码



替代密码(substitution cipher)的原理可用一个例子来说明。（密钥是 3）

明文	abcdefghijklmnopqrstuvwxyz
密文	DEFGHIJKLMNOPQRSTUVWXYZABC

caesar cipher → **FDHVDU FLSKHU**

明文 e 变成了密文 H

置换密码

置换密码(transposition cipher)则是按照某一规则重新排列消息中的比特或字符顺序。

密钥	CIPHER
顺序	145326
明文	attack
	begins
	atfour

根据英文字母在 26 个字母中的先后顺序，我们可以得出密钥中的每一个字母的相对先后顺序。因为密钥中没有 A 和 B，因此 C 为第 1。同理，E 为第 2，H 为第 3, ……，R 为第 6。于是得出密钥字母的相对先后顺序为 145326。

置换密码

置换密码(transposition cipher)则是按照某一规则重新排列消息中的比特或字符顺序。

密钥	CIPHER
顺序	145326
明文	attack
	begins
	atfour

根据英文字母在 26 个字母中的先后顺序，我们可以得出密钥中的每一个字母的相对先后顺序。因为密钥中没有 A 和 B，因此 C 为第 1。同理，E 为第 2，H 为第 3, ……，R 为第 6。于是得出密钥字母的相对先后顺序为 145326。

置换密码

置换密码(transposition cipher)则是按照某一规则重新排列消息中的比特或字符顺序。

密钥	CIPHER
顺序	145326
明文	attack
	begins
	atfour

根据英文字母在 26 个字母中的先后顺序，我们可以得出密钥中的每一个字母的相对先后顺序。因为密钥中没有 A 和 B，因此 C 为第 1。同理，E 为第 2，H 为第 3, ……，R 为第 6。于是得出密钥字母的相对先后顺序为 145326。

置换密码

置换密码(transposition cipher)则是按照某一规则重新排列消息中的比特或字符顺序。

密钥	CIPHER
顺序	145326
明文	attack
	begins
	atfour

根据英文字母在 26 个字母中的先后顺序，我们可以得出密钥中的每一个字母的相对先后顺序。因为密钥中没有 A 和 B，因此 C 为第 1。同理，E 为第 2，H 为第 3, ……，R 为第 6。于是得出密钥字母的相对先后顺序为 145326。

置换密码

置换密码(transposition cipher)则是按照某一规则重新排列消息中的比特或字符顺序。

密钥	CIPHER
顺序	145326
明文	attack
	begins
	atfour

根据英文字母在 26 个字母中的先后顺序，我们可以得出密钥中的每一个字母的相对先后顺序。因为密钥中没有 A 和 B，因此 C 为第 1。同理，E 为第 2，H 为第 3, ……，R 为第 6。于是得出密钥字母的相对先后顺序为 145326。

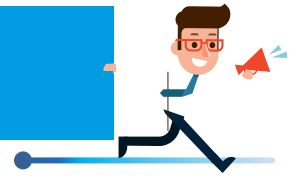
置换密码

置换密码(transposition cipher)则是按照某一规则重新排列消息中的比特或字符顺序。

密钥	CIPHER
顺序	145326
明文	attack
	begins
	atfour

根据英文字母在 26 个字母中的先后顺序，我们可以得出密钥中的每一个字母的相对先后顺序。因为密钥中没有 A 和 B，因此 C 为第 1。同理，E 为第 2，H 为第 3, ……，R 为第 6。于是得出密钥字母的相对先后顺序为 145326。

密文的得出



密钥	CIPHER
顺序	145326
明文	attack
	begins
	atfour

先读顺序为 1 的明文列，即 aba

密文的得出

密钥	CIPHER
顺序	145326
明文	attack
	begins
	atfour

再读顺序为 2 的明文列，即 cnu

密文的得出

密钥	CIPHER
顺序	145326
明文	attack
	begins
	atfour

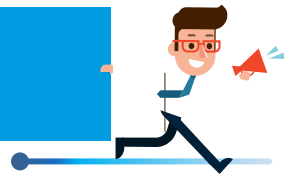
再读顺序为 3 的明文列，即 aio

密文的得出

密钥	CIPHER
顺序	145326
明文	attack
	begins
	atfour

再读顺序为 4 的明文列，即 tet

密文的得出



密钥	CIPHER
顺序	145326
	attack
明文	begins
	atfour

再读顺序为 5 的明文列，即 tgf

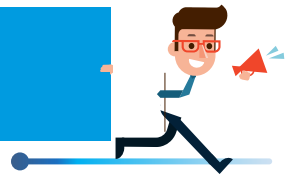
密文的得出

密钥	CIPHER
顺序	145326
明文	attack
	begins
	atfour

最后读顺序为 6 的明文列，即 ksr

因此密文就是：abacnuaiotettgfksr

接收端收到密文后按列写下

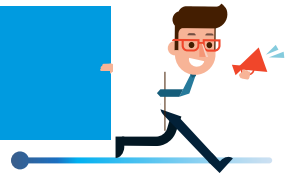


收到的密文：abacnuaiotettgfksr

密钥	CIPHER
顺序	145326
明文	a
	b
	a

先写下第 1 列密文 aba

接收端收到密文后按列写下

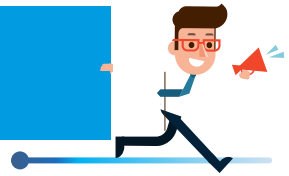


收到的密文：abacnuaiotettgfksr

密钥	CIPHER
顺序	145326
明文	a c b n a u

再写下第 2 列密文 cnu

接收端收到密文后按列写下

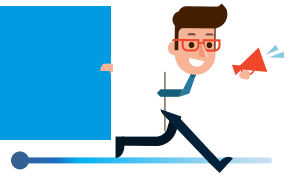


收到的密文：abacnuaiotettgfksr

密钥	CIPHER
顺序	145326
明文	a ac b in a ou

再写下第 3 列密文 aio

接收端收到密文后按列写下



收到的密文：abacnuaictetgfksr

密钥	CIPHER
顺序	145326
明文	at ac be in at ou

再写下第 4 列密文 tet

接收端收到密文后按列写下

收到的密文：abacnuaiotettgfksr

密钥	CIPHER
顺序	145326
明文	attac
	begin
	atfou

再写下第 5 列密文 tgf

接收端收到密文后按列写下

收到的密文：abacnuaiotettgfksr

密钥	CIPHER
顺序	145326
明文	attack
	begins
	atfour

最后写下第 6 列密文 ksr

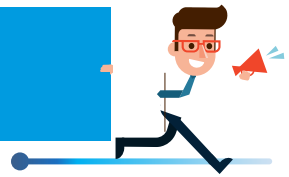
接收端从密文解出明文

收到的密文：abacnuaiotettgfksr

密钥	CIPHER
顺序	145326
明文	attack begins atfour

最后按行读出明文

接收端从密文解出明文

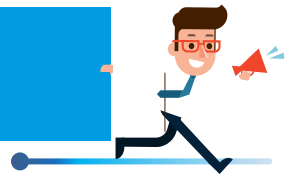


收到的密文：abacnuaiotettgfksr

密钥	CIPHER
顺序	145326
明文	attack begins atfour

最后按行读出明文

接收端从密文解出明文

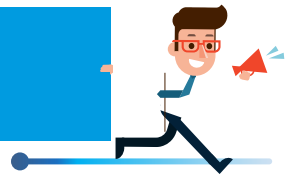


收到的密文：abacnuaiotettgfksr

密钥	CIPHER
顺序	145326
明文	attack begins atfour

最后按行读出明文

接收端从密文解出明文



收到的密文：abacnuaiotettgfksr

密钥	CIPHER
顺序	145326
明文	attack begins atfour

最后按行读出明文

得出明文：attack begins atfour