石家莊鐵道大學
SHIJIAZHUANG TIEDAO UNIVERSITY

在线开放课程

电子商务技术基础

电子商务安全技术--1

主讲 ： 赵宁

目录

电子商务安全问题

- ✓ 电子商务安全可划分为计算机物理安全、计算机网络安全和商务交易安全等。
- ✓ 计算机物理安全包括计算机的异常损毁、被盗、非法使用等，常用的安全技术有系统备份、系统加密等。
- ✓ 计算机网络安全包括计算机网络设备安全、计算机网络系统安全、数据库安全等。常用的安全措施有防火墙、防病毒软件、入侵检测等。

电子商务安全问题

- ✓ 商务交易安全则是指传统商务在互联网络上应用时产生的各种安全问题，主要有交易信息的机密性、真实性、可控性、可用性。
- ✓ 商务交易安全的主要安全技术是加密和认证。交易安全是建立在计算机网络安全基础之上的。

常见威胁和攻击类型

- ✓ 非技术性攻击：用诡计或其他形式骗取人们暴露敏感信息或执行一个危及网络安全的行为。
- ✓ 拒绝服务攻击：攻击者使用某特定软件向目标计算机发送大量的数据包使其资源过载而无法提供正常服务。

常见威胁和攻击类型

- ✓ 恶意代码攻击：通过一定的传播途径将非法的、具有破坏性的程序安放在个人计算机或某个网络服务器上，当触发该程序运行的条件满足时，如果打开个人计算机或访问该网络服务器，就会使该程序运行从而产生破坏性结果。主要的恶意代码有蠕虫、特洛伊木马等。

电子商务的安全要素

1. 有效性
   真实性
2. 机密性
3. 完整性
4. 可靠性
   不可抵赖性可控性
5. 审查能力
6. 鉴别另一方的身份(认证性)

电子商务的安全体系

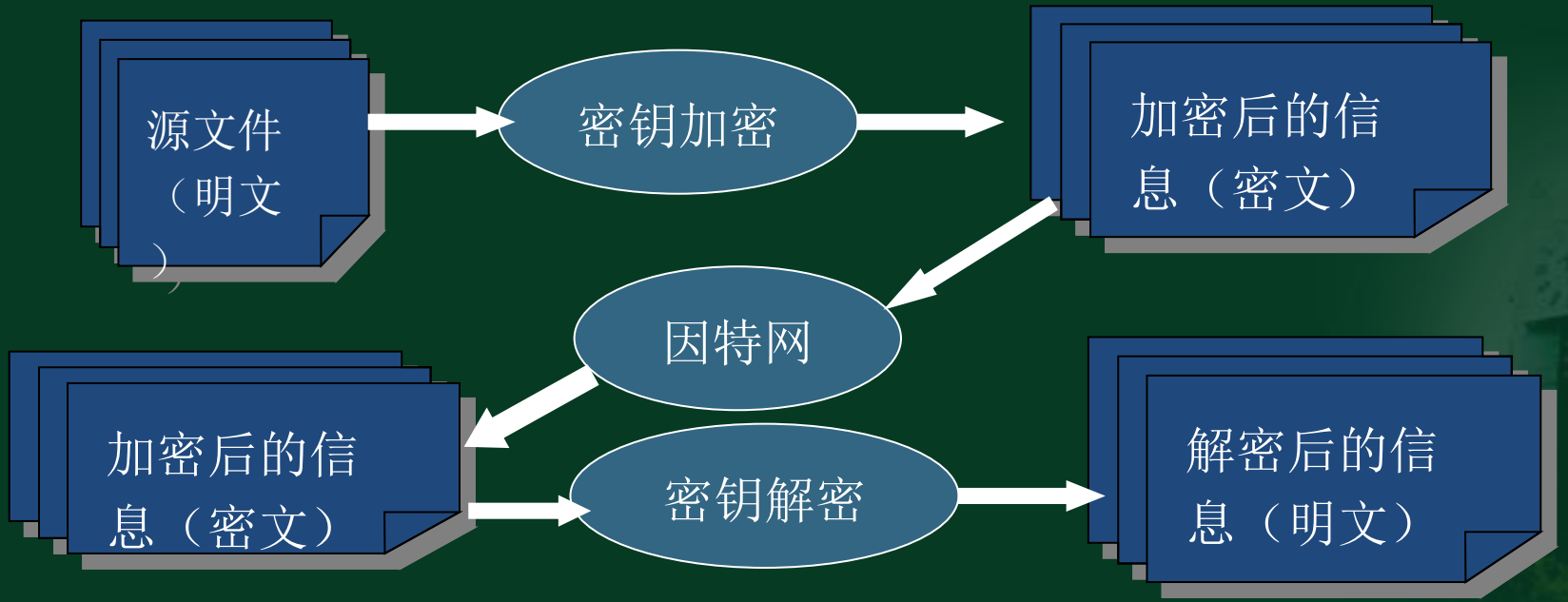
电子商务安全要素：真实性、机密性、完整性、可靠性、不可 抵赖性等
商务系统层：各种商务应用系统（Ｂ２Ｂ、Ｂ２Ｃ、Ｂ２C等）
交易协议层： SSL协议、SET协议、S-HTTP协议等
安全认证层：数字签名、数字时间戳、数字证书、CA认证
加密技术层：对称加密（ＤＥＳ）、非对称加密（ＲＳＡ）等
网络服务层：网络隐患扫描、网络安全监控、内容识别、访问控制、防火墙等

电子商务安全构架

交易安全技术	电子商务安全体系	网络安全技术
安全应用协议 （SET、SSL） 安全认证手段 （数字签名、CA体系） 基本加密算法 （对称和非对称加密算法）		病毒防范 身份识别技术 防火墙技术 虚拟专用网
法律法规、政策		

加密系统

- 加密技术是最基本的安全技术，是实现信息保密性的一种重要手段，其目的是为了防止非法用户获取信息系统中的机密信息。



几种常见的加密体制技术实现：

- 一替换加密法：
- 1. 单字母加密法
  - 例一：Caesar（恺撒）密码
  - 例二：将字母倒排序
  - 例三：单表置换密码
- 2. 多字母加密法
  - 例一：Vigenere密码
  - 例二：转换加密

单字母加密方法

例 1：Caesar（恺撒）密码，见表 1。

表 1　　Caesar（恺撒）密码表

明文字母	a	b	c	d	e	f	g	h	i	j	k	l	m
密文字母	D	E	F	G	H	I	J	K	L	M	N	O	P

明文字母	n	o	p	q	r	s	t	u	v	w	x	y	z
密文字母	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

例：明文（记做m）为“important” 则密文（记做C）则为“LPSRUWDQW”。

单字母加密方法

表 2　　字母倒排序

明文字母	a	b	c	d	e	f	g	h	i	j	k	l	m
密文字母	Z	Y	X	W	V	U	T	S	R	Q	P	O	N

明文字母	n	o	p	q	r	s	t	u	v	w	x	y	z
密文字母	M	L	K	J	I	H	G	F	E	D	C	B	A

例：如果明文m为“important”，则密文C则为“RNKLIGZMZ”。

单字母加密方法

例3：单表置换密码，见表3。

假设密钥Key是BEIJINGTSINGHUA（北京清华），由此密码构造的字符置换表如下：

表 3　　单表置换密码

明文字母	a	b	c	d	e	f	g	h	i	j	k	l	m
密文字母	B	E	I	J	N	G	T	S	H	U	A	C	D
明文字母	n	o	p	q	r	s	t	u	v	w	x	y	z
密文字母	F	K	L	M	O	P	Q	R	V	W	X	Y	Z

例：如果明文m为“important”，则密文C则为“HDLKOQBFQ”。

多字母加密方法--vigenere加密

- 多字母加密是使用密钥进行加密。密钥是一组信息（一串字符）。同一个明文经过不同的密钥加密后，其密文也会不同
- 例1：Vigenere密码，见表4。加密方法如下：
  - 假设明文m=m1m2m3.....mn，
  - 密钥Key=K1K2K3.....Kn，
  - 对应密文C=C1C2C3.....Cn，
  - 则：Ci = mi + Ki mod 26，i = 1，2，...n，

多字母加密方法--vigenere加密

- 其中，26个字母A----Z的序号对应是0----25
- Ci 是密文中第i个字母的序号，
- mi 是明文中第i个字母的序号，
- Ki 是密钥Key中第i个字母的序号，
- 如果m=information
- Key=STAR　　则C=AGFFJFAKAHN　如i=8,s=18;

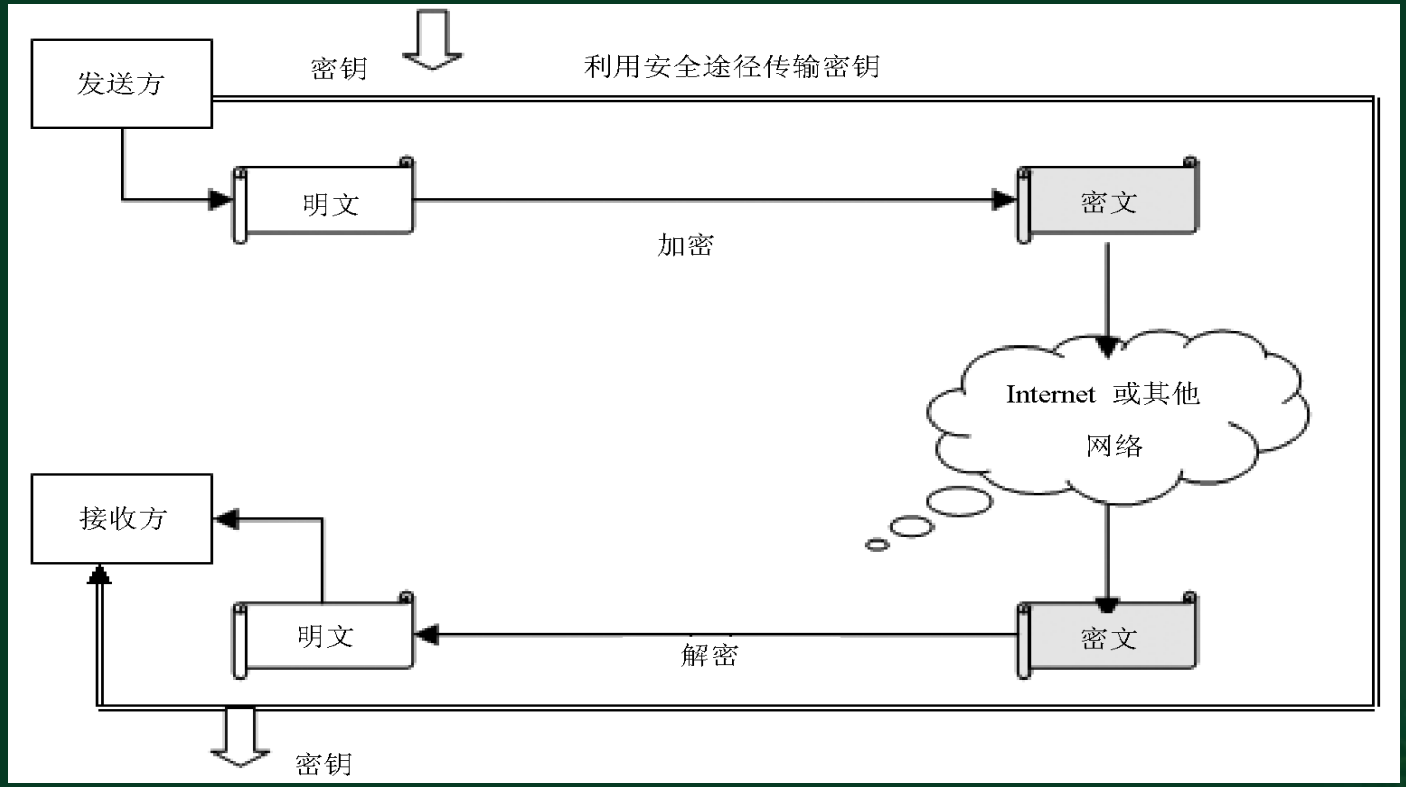
多字母加密---转换加密法

- 替换加密法中，原文的顺序没改变，而是通过各种字母映射关系把原文隐藏起来。转换加密法是将原字母的顺序打乱，将其重新排列。
- 如：it can allow students to get close up views
- 将其按顺序分为5个字符的字符串：
- itcan allow stude ntsto
- 将其按先列后行的顺序排列，就形成密文为：
- “IASNGOVTLTTESICLUSTEEAODTCUWNWEOLPS”

加密算法--对称密钥加密算法DES

- 对称密钥加密标准DES（Data Encryption Standard）算法是美国国家标准化局NBS（National Bureau of Standard）于1976年11月23日作为一个官方的联邦标准颁布的。这种加密算法被规定用于所有的公开场合或私人的保密通讯领域，后来该算法被ISO接受为国际标准。
- DES算法是将两种基本的加密算法（替换加密和转换加密）完美地结合起来。

对称加密体系制加密流程示意图



加密算法—非对称加密

- 非对称密钥加密技术

  非对称加密又称为公开密钥加密，与对称密钥系统相比，公开密钥加密技术需要使用一对相关的密钥：一个用来加密，另一个用来解密。

- 公开密钥系统的基本模式：
  - 加密模式(接收方的公钥发，私钥解)

RSA加密算法

- 该算法于1977年由三位年轻教授提出并以三人的姓氏命名为RSA算法。
- 该算法利用了把两个大质数相乘生成一个合数是容易的，但要把一个合数分解为两个质数却困难。合数分解问题目前仍然是数学领域尚未解决的一大难题。
- RSA是公钥密码体制中的一种，RSA的算法如下：

RSA加密算法

（1）选取两个足够大的质数P和Q；

（2）计算P和Q相乘所产生的乘积n=P×Q；

（3）找出一个小于n的数e，使其符合与(P－1)×（Q－1）无公共因子；

（4）另找一个数d，使其满足（e×d）mod [（P－1）×（Q－1）]=1；

（5）(n，e)为公开密钥，(n，d)为私有密钥；

（6）加密和解密的运算方式为：设m为明文，

加密：密文c=m^e（mod n）

解密：明文m=c^d（mod n）

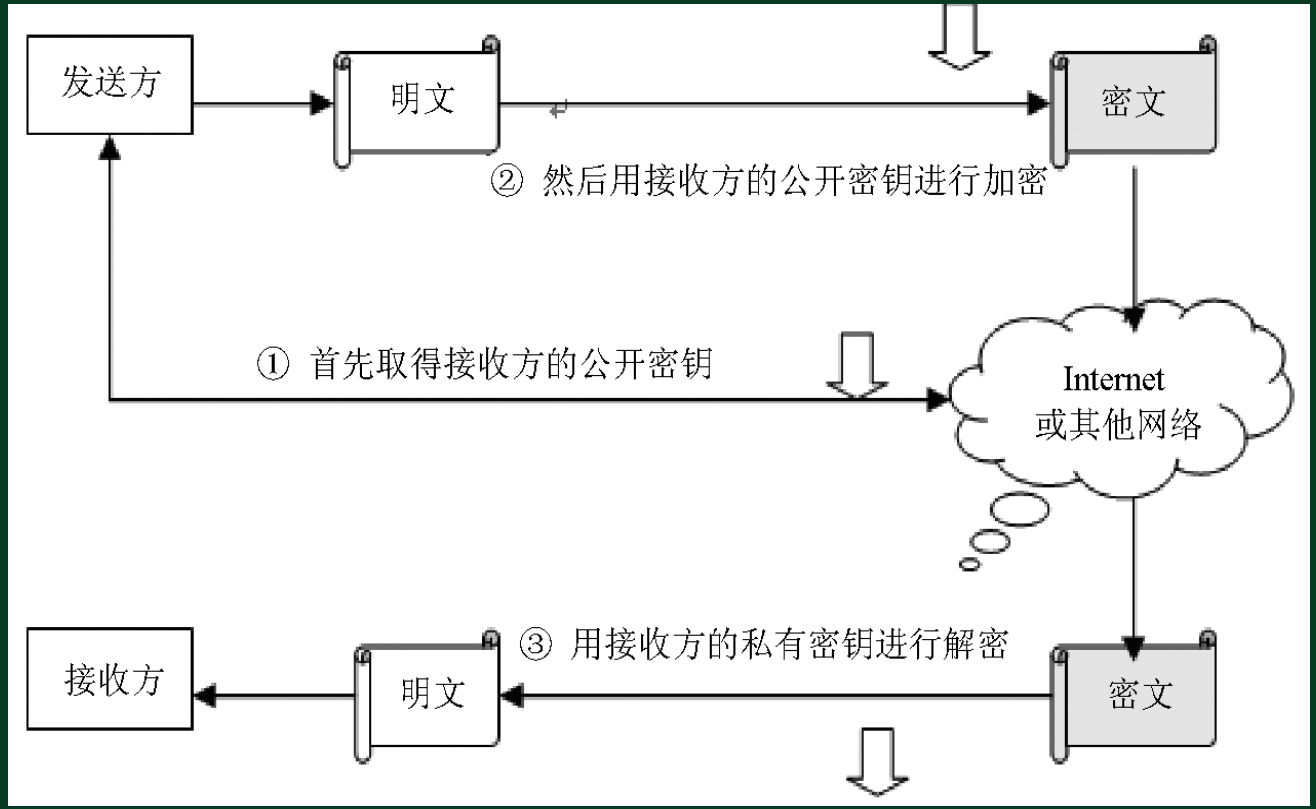
RSA加密算法

假定P ＝3，Q ＝11，则n = P×Q ＝33，选择e =3，因为3和20没有公共因子。（3×d）MOD（20）＝1，得出d=7。从而得到（33，3）为公钥；（33，7）为私钥。加密过程为将明文M的3次方模33得到密文C，解密过程为将密文C 的7次方模33得到明文。下表显示了非对称加密和解密的过程。

RSA加密算法

明文 M			密文 C		解密	
字母	序号	M^3	M^3（MOD 33）	C^7	C^7（MOD 33）	字母
A	01	1	01	1	01	A
E	05	125	26	8031810176	05	E
N	14	2744	05	78125	14	N
S	19	6859	28	13492928512	19	S
Z	125261	17576	20	128000000	26	Z

非对称加密的工作流程示意图



小结

- 本部分首先总体分析了电子商务安全要素及安全体系、安全威胁，后重点分析了加密：加密技术：单字母加密和多字母加密；加密算法：对称加密和非对称加密各自的工作流程。