《现代密码学》第一讲

绪　论

参考书目

- 《现代密码学教程》，谷利泽等，北邮出版社，2009
- 现代密码学基础，章照止，北邮出版社，2004
- 现代密码学，杨波，清华大学出版社，2004

参考书目

- **密码学原理与实践**, (加)Douglas R.Stinson 著，冯登国 译，电子工业出版社，2003.
- **密码编码学与网络安全——原理与实践**,(美) Stallings,W. 著，孟庆树 等译,电子工业出版社,2006.
- **应用密码学－协议、算法与C源程序**，Burce等，机械工业出版社，2002.
- **现代密码学理论与实践**，Wenbo Mao著，王继林 译，电子工业出版社，2004.
- 应用密码学手册, **Alfred Menezes** 著，胡磊 译，电子工业出版社，2005
- **密码学基础**，O.Goldreich著，杨义先等译，人民邮电出版社，2003.
- **高级加密标准（AES)算法—Rijndael的设计**，John Daemen, Vincent Rijndael著；谷大武等译，清华大学出版社，2003.

注意事项

- 《现代密码学》是信息安全专业重要的专业基础课，理论性强，难度大，请大家用功学习。

密码学的目的

- 中国古代的保密

例1：汉代泥封

古时的官、私文书和书信往来大都写在竹简或木牍上，这些简牍书信，在传递过程中需要保密就得封缄起来。封缄的方式是把简牍用绳子穿连起来，卷好，在外面加上一枚挖了方槽的木块(即封泥匣)，再用绳子把它和简牍一起绑好，用一团软泥捺在方槽里的绳子上，然后用印章在泥上按捺出印文，以防私拆。后来随着纸的出现，木块为信封取代，封泥印发展到后来就变成火漆印。

例2：雍正密折制度

明朝的时候，大臣上奏给皇帝的奏折，通过各级衙门层层上报，有时皇帝没看到奏章，一些大臣已经知道奏章的内容。为了加强保密，雍正时期开始使用这种奏折匣，它配以宫廷特制铜锁。只有皇帝和上奏的大臣才有钥匙。大臣上奏的密折除了皇帝之外，任何人无法知晓。

密码学的目的

- 中国古代的认证

例1：《水浒转》第三十九回“梁山泊戴宗传假信”

金大坚，善刻当时的苏、黄、米、蔡四种字体。宋江被捉关在江州，吴用献计，把圣手书生萧让和玉臂匠金大坚请上梁山，金大坚刻了蔡京的假印，用来骗蔡京。不小心刻了蔡京的名讳图章。

哪有老子给儿子写信，盖自己名讳图章的呢？此事被黄文炳看破，险些断送了宋江、戴宗的性命。

例2：字画鉴别

有一回在某拍卖会上，一幅“溥杰”的书法被指为赝品！拍卖会现场有人说：此瘦金体写得如何姑且不论，这章子就大错特错了。

其实，古人在写字时的落款和钤印，非常讲究“规矩”。溥杰的钤印除“溥杰”之外最喜“用笔在心”、“闲可挥毫”等闲章。此画“闲章”居然刻着：“梦回白山黑水”，可见是不熟悉溥杰的人的伪作。

例 3：接头暗号

《鹿鼎记》中反清复明的暗号语。 上句：“地振高冈，一派溪山千古秀。”下句就对：“门朝大海，三河合水万年流。”

攻击的主要形式

- 中断（Interruption）：DoS/DDoS
- 截取（Interception）:Sniffer/Ethereal
- 篡改（Modification）
- 伪造（Fabrication）:IP欺骗、phishing
- 重放攻击（Replay）:利用协议漏洞（如身份认证协议等、密钥交换/分配协议等）

信息安全的目标

密码学是保障信息安全的核心，信息安全是密码学研究与发展的目的

- 保密性(Confidentiality)
- 完整性(Integrity)
- 认证性(Identity Authentication, MAC/Digital Certification)
- 不可否认性(Digital Signature)
- 可用性(Availability)

密码学的历史

- 滚筒密码（人类有记载的第一个密码）
- 凯撒密码（古罗马古埃及时代）
- 两次世界大战的密码战(Enigma密码机)

Websites about the Enigma cipher machine

- Cipher Machines & Cryptology (Enigma simulator website)

http://users.telenet.be/d.rijmenants

- Paul Reuvers' and Marc Simoens' Cryptomuseum

www.cryptomuseum.com

- Bletchley Park official site:

www.bletchleypark.org.uk

- Tom Perera's Enigma Museum:

http://w1tp.com/enigma

- Frode Weierud's Crypto Cellar

http://cryptocellar.org

- David Hamer's cryptology website:

http://home.comcast.net/~dhhamer

- Tony Sale's Enigma pages:

www.codesandciphers.org.uk/enigma

密码学的历史

Shannon,1949 “*Communication Theory of Secrecy System* “

- 1976 美国国家标准局(NBS)　DES
- 1976 Diffie-Hellman “*New Direction in Cryptography* ”
- 1997 美国标准技术协会(NIST)　AES
- 社会信息化催化民用（商用）密码：电子商务、电子政务、网络银行、网络邮局。。。
- 2004年8月28日　“中华人民共和国电子签名法”

密码学的分类

- 传统密码
  - 古代密码术：隐写术
  - 代换（substitution）密码
  - 置换（Permutation）密码
- 现代密码学
  - 序列密码（流密码）
  - 对称密码体制
  - 非对称密码体制

密码学新动向

- 密码算法设计新思路
  - DNA密码
  - 量子密码

密码学基础

I. 理论基础:Number theory, Algebra，Discrete Mathematics, Concrete Mathematics, complexity theory, Information Theory, Computer Science.

密码学基础

II. 现代密码学:

A. Symmetrical cryptology: Sequential cipher/stream cipher/Block cipher

实现机密性

B. Asymmetric Cryptology: RSA/ECC

实现数字签名/数字证书/不可否认性/MAC(完整性)

C. Key management: 生成、分发、注销、更新…

密码学基础

III. 现代密码学应用:

A. 认证技术：身份认证

B. Network security Protocol(IPv4的各层，IPv6)

C. Access Control: Role-Based/Discretionary Mandatory/Access Control(RBAC,DAC,MAC)

密码学基本术语

- 密码学(Cryptology)：研究信息系统安全保密的科学。它包含两个分支:
  - ✓密码编码学(Cryptography)，对信息进行编码实现隐蔽信息的一门学问。
  - ✓密码分析学(Cryptanalytics)，研究分析破译密码的学问。

密码学基本术语

- 明文(消息)(Plaintext) ：被隐蔽消息。
- 密文(Ciphertext)或密报(Cryptogram)：明文经密码变换成的一种隐蔽形式。
- 加密(Encryption)：将明文变换为密文的过程。
- 解密(Decryption)：加密的逆过程，即由密文恢复出原明文的过程。
- 加密员或密码员(Cryptographer)：对明文进行加密操作的人员。

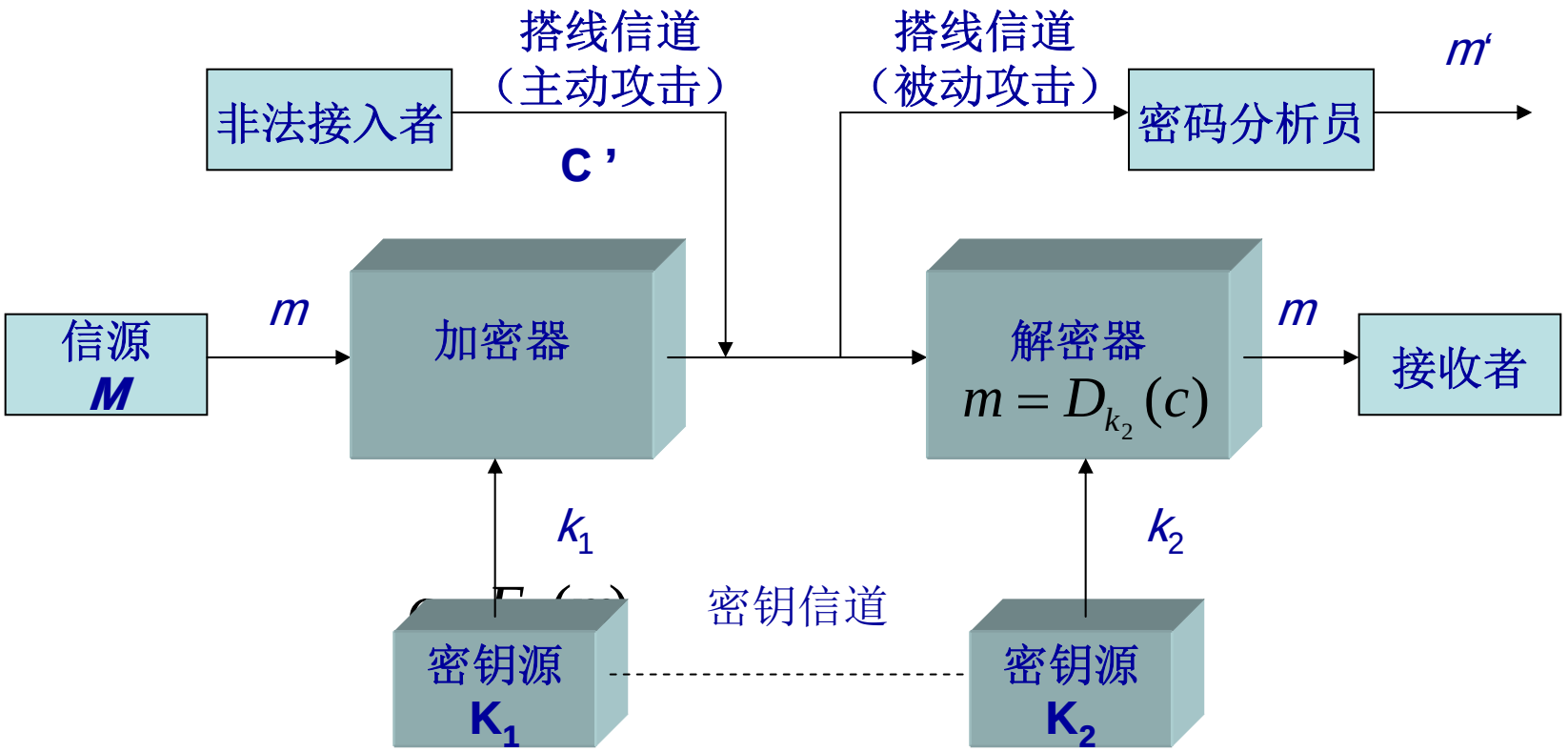
密码学基本术语

- 加密算法(Encryption algorithm)：密码员对明文进行加密时所采用的一组规则。
- 接收者(Receiver)：传送消息的预定对象。
- 解密算法(**Decryption algorithm**)：接收者对密文进行解密时所采用的一组规则。
- 密钥(Key)：控制加密和解密算法操作的数据处理，分别称作加密密钥和解密密钥。
- 截收者(Eavesdropper)：在信息传输和处理系统中的非受权者，通过搭线窃听、电磁窃听、声音窃听等来窃取机密信息。

密码学基本术语

- 密码分析(Cryptanalysis)：截收者试图通过分析从截获的密文推断出原来的明文或密钥。
- 密码分析员(Cryptanalyst)：从事密码分析的人。
- 被动攻击(Passive attack)：对一个保密系统采取截获密文进行分析的攻击。
- 主动攻击(Active attack)：非法入侵者(Tamper)、攻击者(Attacker)或黑客(Hacker)主动向系统窜扰，采用删除、增添、重放、伪造等窜改手段向系统注入假消息，达到利已害人的目的。

保密通信系统的模型



保密通信系统模型

密码体制分类

密码体制从原理上可分为两大类，即：

- 单钥体制(Symmetric System, One-key System, Secret-key System)
- 双钥体制(Asymmetric System, Two-key System, Public-key System)。

单钥体制对明文消息的加密有两种方式： 一是明文消息按字符（如二元数字）逐位地加密，称之为流密码(**StreamCipher**)；另一种是将明文消息分组（含有多个字符），逐组地进行加密，称之为分组密码(**block cryptography**)。

密码体制分类

双钥体制是由**Diffie**和**Hellman**于**1976**年首先引入的。

采用双钥体制的每个用户都有一对选定的密钥：一个是可以公开的，可以像电话号码一样进行注册公布；另一个则是秘密的。因此双钥体制又称为公钥体制。

双钥密码体制的主要特点是将加密和解密能力分开，因而可以实现多个用户加密的消息只能由一个用户解读（机密性），或由一个用户加密的消息而使多个用户可以解读（数字签名）。无需事先分发密钥。

密码体制的安全性

- 无条件安全（理论安全性）

只有一次一密的密码体制，即key至少要和plaintext长度是一样的才是无条件安全。（流密码）

- 有条件安全性（实际安全性）

根据破解密码系统的计算量来评价其安全性

- 计算安全性：已知算法和计算工具不可能完成破解要求完成的计算量。
- 实际安全性：破解成本超过了加密信息本身的价值或所花时间超过了加密信息的时效期。
- 可证明安全性：将密码系统的安全性归结为尚未解决的数学难题

1.3.3 密码攻击概述

攻击类型	攻击者拥有的资源
惟密文攻击	•加密算法 •截获的部分密文
已知明文攻击	•加密算法， •截获的部分密文和相应的明文
选择明文攻击	•加密算法 •截获的部分密文 •自己选择的明文消息及由密钥产生的相应密文
选择密文攻击	•加密算法 •截获的部分密文 •自己选择的密文消息及相应的被解密的明文

明文中各个字母出现的统计概率

Letter	Frequency	Letter	Frequency	Letter	Frequency
e	12.31%	l	4.03%	b	1.62%
t	9.59%	d	3.65%	g	1.61%
a	8.05%	c	3.20%	v	0.93%
o	7.94%	u	3.10%	k	0.52%
n	7.19%	p	2.29%	q	0.20%
i	7.18%	f	2.28%	x	0.20%
s	6.59%	m	2.25%	j	0.10%
r	6.03%	w	2.03%	z	0.09%
h	5.14%	y	1.88%		

字符出现频率分类

- E，有概率大约0.120。
- T，A，O，I，N，S，H，R，每个有概率在0.06～0.09间。
- D，L，每个有概率大约0.04。
- C，U，M，W，F，G，Y，P，B，每个有概率在0.015～0.023之间。
- V，K，J，X，Q，Z，每个概率少于0.01。
- 当考虑位置特性时，字母A，I和H一般不作为单词的结尾，而E，N和R出现在起始位置比出现在结束位置的概率更小，字母T，O和S出现在单词前后位置的概率基本相同。
- 应该强调的是，这些表并不包含结论性的信息。字母的分布大大依赖于明文文本的类型：诗歌，标语，科技等等，所以有些出入也是正常的。

字母组合概率(递减)

- 双字母组合：TH，HE，IN，ER，AN，RE，DE，ON，ES，ST，EN，AT，TO，NT，HA，ND，OU，EA，NG和AS。
- 三字母组合：THE，ING，AND，HER，ERE，ENT，THA，NTH，WAS和ETH。

Word	Frequency	Word	Frequency	Word	Frequency
the	6.421%	a	2.092%	i	0.945%
of	4.028%	in	1.778%	it	0.930%
and	3.150%	that	1.244%	for	0.770%
to	2.367%	is	1.034%	as	0.764%

十个最常用中文单字频率

政　治		文　艺		新　闻		科　技		综　合	
字	频率	字	频率	字	频率	字	频率	字	频率
的	0.0536	的	0.0324	的	0.0375	的	0.0320	的	0.0384
是	0.0165	一	0.0218	一	0.0132	一	0.0097	一	0.0125
一	0.0136	了	0.0196	了	0.0120	在	0.0092	是	0.0098
在	0.0115	不	0.0165	和	0.0086	用	0.0079	在	0.0095
这	0.0109	是	0.0141	在	0.0086	有	0.0073	了	0.0082
主	0.0108	说	0.0130	人	0.0083	是	0.0070	不	0.0081
不	0.0101	他	0.0130	大	0.0083	不	0.0069	和	0.0075
和	0.0098	这	0.0119	主	0.0083	中	0.0066	有	0.0069
人	0.0087	着	0.0107	是	0.0078	大	0.0064	的	0.0069
们	0.0087	个	0.0097	们	0.0065	时	0.0063	这	0.0064

唯密文攻击举例：

卡西斯基(Kasiski)测试法

基本原理：若用给定的k个密钥表周期地对明文字母加密，则当明文中有两个相同字母组在明文序列中间隔的字母数为k的倍数时，这两个明文字母组对应的密文字母组必相同。但反过来，若密文中出现两个相同的字母组，它们所对应的明文字母组未必相同，但相同的可能性很大。如果我们将密文中相同的字母组找出来，并对其相同字母数综合研究，找出它们的相同字母数的最大公因子，就有可能提取出有关密钥字的长度k的信息。

唯密文攻击举例：

举例(密文)

CHREEVOAHMAERATBIAXXWTNXBEEOPHBSBQMQ
EQERBWRVXUOAKXAOSXXWEAHBWGJMMQMNKGR
FVGXWTRZXWIAKLXFPSKAUTEMNDCMGTSXMXBTUI
ADNGMGPSRELXNJELXVRVPRTULHDNQWTWDTYG
BPHXTFALJHASVBFXNGLLCHRZBWELEKMSJIKNBH
WRJGNMGJSGLXFEYPHAGNRBIEQJTAMRVLCRREM
NDGLXRRIMGNSNRWCHRQHAEYEVTAQEBBIPEEWE
VKAKOEWADREMXMTBHHCHRTKDNVRZCHRCLQOH
PWQAIIWXNRMGWOIIFKEE

唯密文攻击举例：

估算密钥字的长度

可以看出，密文片段CHR在密文中出现了5次，每次出现的开始位置分别为1，166，236，276，286。第一次出现的距离分别为为165，235，275，285。容易计算：gcd(165,235,275,285)=5。

因此，密钥字的长度很可能是5。

唯密文攻击举例：

重合指数法的引入

- 如果我们考虑一个来自26个字母表的完全随机文本，则每个字母有同样的概率发生，等于1/26。假定我们另有第二个随机文本，把它放在第一个下面，然后我们计算有多大的机会找到上下两个字母相等。因为每个字母都是一个随机字符，找到两个都是的概率是$(1/26)^2$。显然，对于其他字母而言这个概率是不变的，所以找到两个同样字母的总的概率是：$26(1/26)^2=1/26=0.0385$。
- 对英语文本，与随机文本不同，我们发现字母发生的概率是不同的。设字母A、B、...Y、Z出现的期望概率分别为p_0、p_1、...p_{24}、p_{25}，此时找到两个等同字母发生的概率为：$\sum_{i=0}^{25} p_i^2 = 0.065$。这个值比随机文本的情况大得多。我们把它称之为重合指数。

唯密文攻击举例：

重合指数法的含义及计算方法

- 设某种语言由个n字母组成，每个字母i发生的概率为 $p_i, 1 \le i \le n$，则重合指数就是指两个随机字母相同的概率，记为：$IC = \sum_{i=1}^{n} p_i^2$ 。
- 由于现实世界中密文的长度有限，故从密文计算的重合指数总是不同于理论值，所以一般用IC的无偏估计值 $IC' = \sum_{i=1}^{n} \frac{x_i(x_i-1)}{L(L-1)}$ 来近似计算IC，IC'公式中 x_i 是密文符号i出现的次数，L指的是密文长度，n表示某门语言包含的字母数，如该语言是英文字母，则n=26。

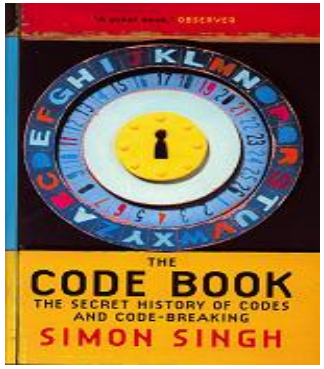
唯密文攻击举例：

利用重合指数估算密钥字长度

密钥字长度	重合指数				
i=1	0.045				
i=2	0.046	0.041			
i=3	0.043	0.050	0.047		
i=4	0.042	0.039	0.046	0.040	
i=5	0.063	0.068	0.069	0.061	0.072

Useful references:

- 威廉姆•斯大林书的电子链接
  - www.williamstallings.com/
- 《The Code Book》作者赛门•辛的链接：www.simonsingh.net

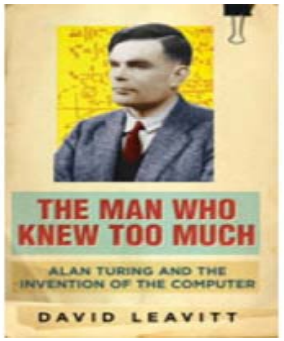


- 影视资料：
  - 破解纳粹的秘密 Decoding Nazi Secrets
  - Code-Breakers(BBC)

Useful references:

- Bletchley Park(二战时期英国密码破译基地柏雷屈里园)
  - www.codesandciphers.org.uk/



- 关于亚伦.图灵
  - www.turing.org.uk/turing (Alan Turing)
- Enigma emulators(奇谜模拟机)
  - http://www.xat.nl/enigma/
  - http://www.ellsbury.com/enigmabombe.htm

Useful references:

- 关于Phil Zimmerman和PGP
  - http://www.philzimmermann.com
    www.pgpi.org
- 量子计算中心
  - www.qubit.org
- 美国国家密码学博物馆 National Security Agency
  - www.nsa.gov/museum
- 美国密码协会ACA
  - http://www.und.nodak.edu/org/crypto/crypto/
- Cryptography FAQ
  - http://www.faqs.org/faqs/cryptography-faq/

- 哈工程马春光教授研究团队
  - http://machunguang.hrbeu.edu.cn