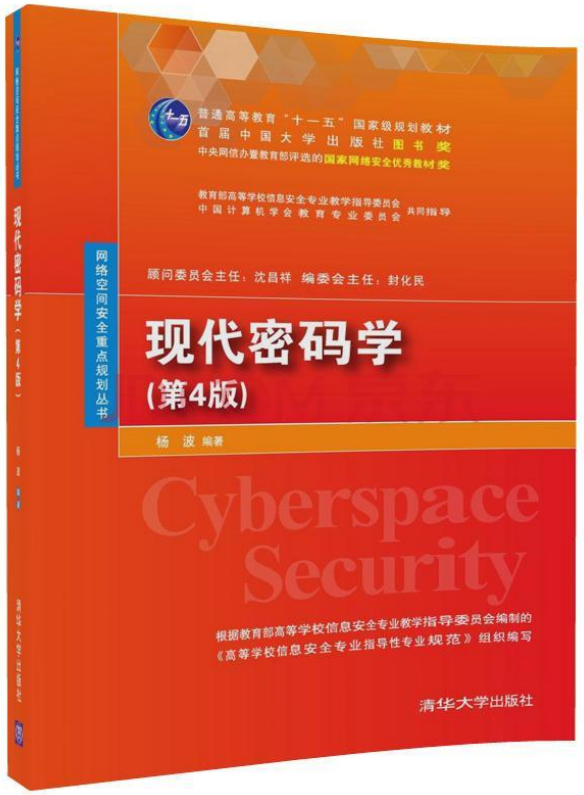
现代密码学

廖永建
电子科技大学 信息与软件工程学院
网络空间安全实验室

简介

- 廖永建
- 博士，副教授
- 研究方向：密码学、公钥密码算法、安全协议、云安全、大数据安全
- 办公地点：沙河校区逸夫楼**338**
- 联系方式：**liaoyj@uestc.edu.cn**

现代密码学（第4版），杨波，清华大学出版社，2017



参考书目

- 现代密码学（第4版），杨波，清华大学出版社，2017
- 密码学导引，冯登国，裴定一，科学出版社，1999。
- 应用密码学手册，[加拿大] 梅尼斯（Menezes） 等著；胡磊，王鹏等译，电子工业出版社，2005。

目录

第1章 引言
第2章 流密码
第3章 分组密码体制
第4章 公钥密码
第5章 杂凑函数
第6章 数字签名
第7章 密码协议

第一章 引言

- 什么是安全？
- 外国古代密码艺术
- 中国古代密码艺术
- 密码学基本概念
- 密码分析学
- 古典密码体制

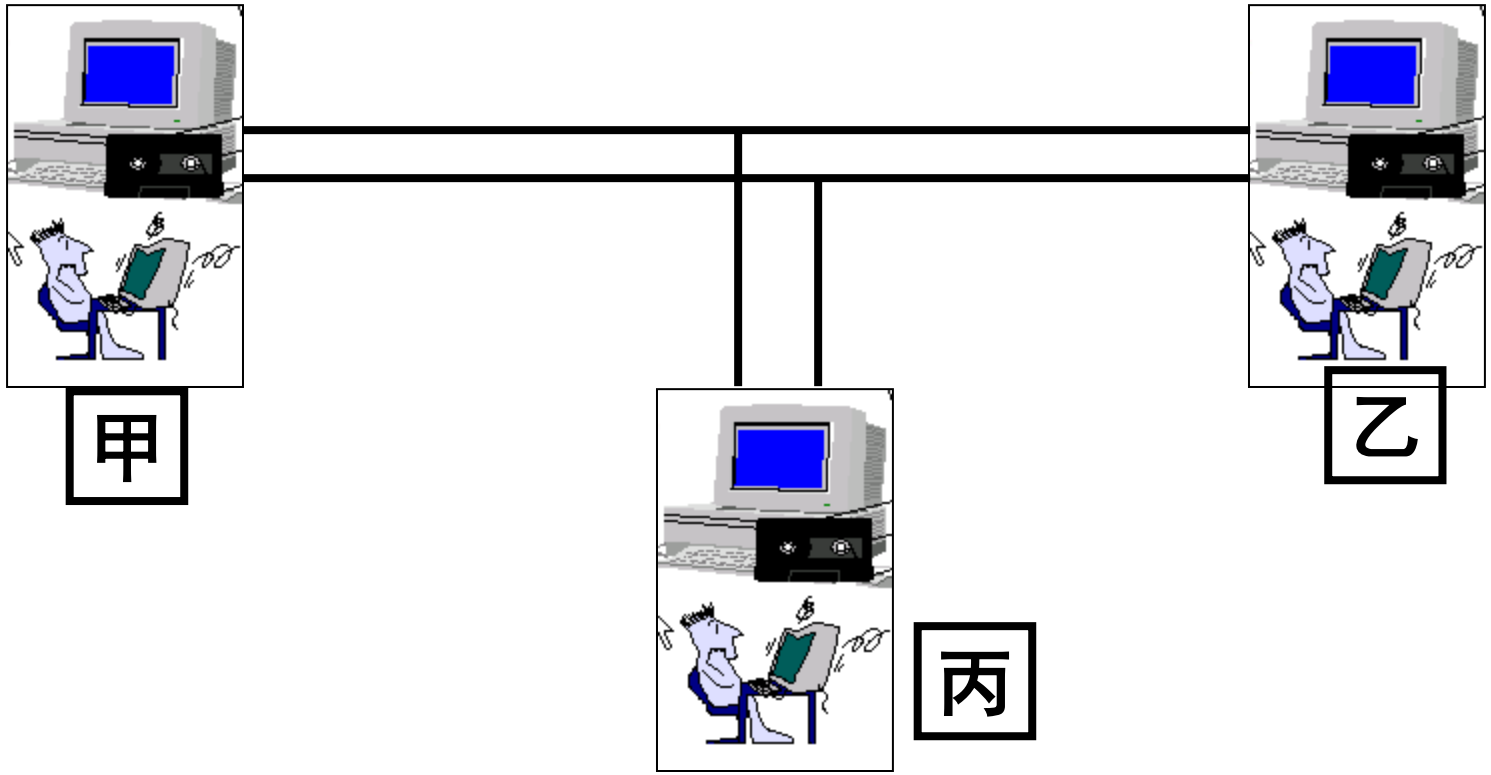
什么是安全？

- **“安全”的含义（Security or Safety?）**

  平安，无危险；保护，保全；

  远离危险的状态或特性；

信息安全的基本任务



安全威胁

攻击的分类：

1. 被动攻击

2. 主动攻击

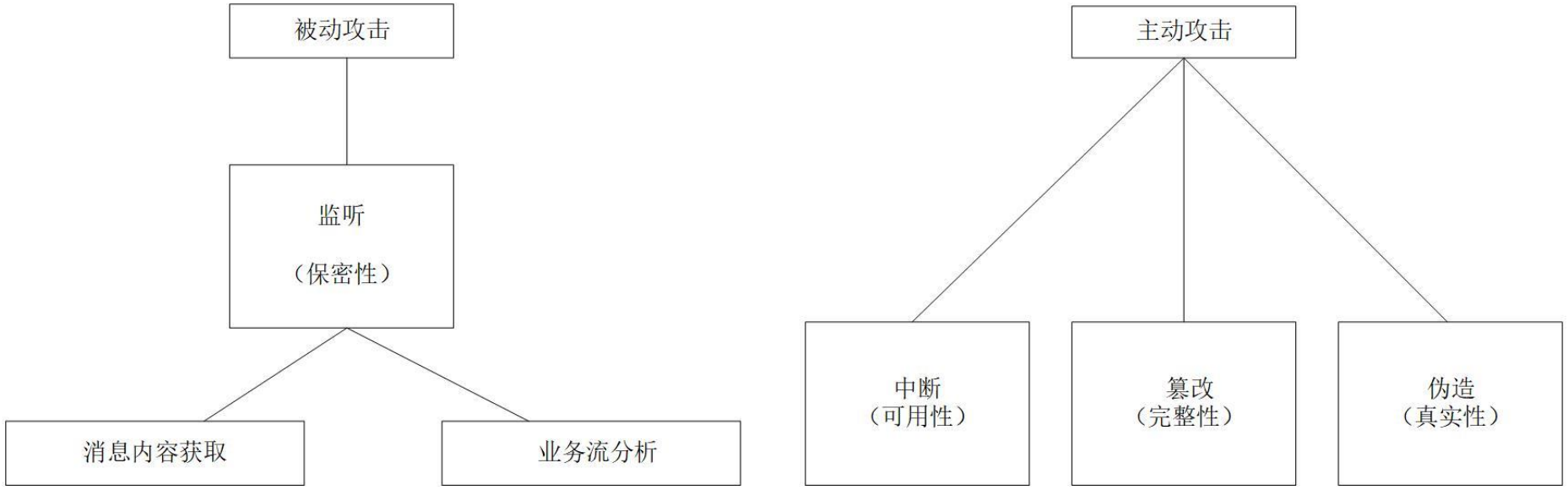


图1.1 攻击分方式特点

信息安全的基本属性

- 机密性
- 可用性
- 完整性
- 认证
- 不可否认性
- 访问控制
- 。。。

信息安全的基本属性（续）

- 机密性 **Confidentiality**
  - 保证信息为授权者享用而不泄漏给未经授权者。
  - 别人“看不到”或“看不懂”
- 可用性 **Availability**
  - 保证信息和信息系统随时为授权者提供服务，而不要出现非授权者滥用却对授权者拒绝服务的情况。
  - 想看的时候是“可以看到的”
- 完整性 **Integrity**
  - 数据完整性，未被未授权篡改或者损坏
  - 系统完整性，系统未被非授权操纵，按既定的功能运行
  - 信息没有被“动过”

信息安全的基本属性（续）

- 认证（**Authentication**）
  - 消息认证，保证消息来源的真实性
  - 身份认证，确保通信实体的真实性
- 信息的不可否认性（**Non-repudiation** ）
  - 要求无论发送方还是接收方都不能抵赖所进行的传输
- 可靠性（**Reliability**）
  - 特定行为和结果的一致性
- 可控性
  - 授权实体可以控制信息系统和信息使用的特性
- 审计（**Accountability**）
  - 确保实体的活动可被跟踪

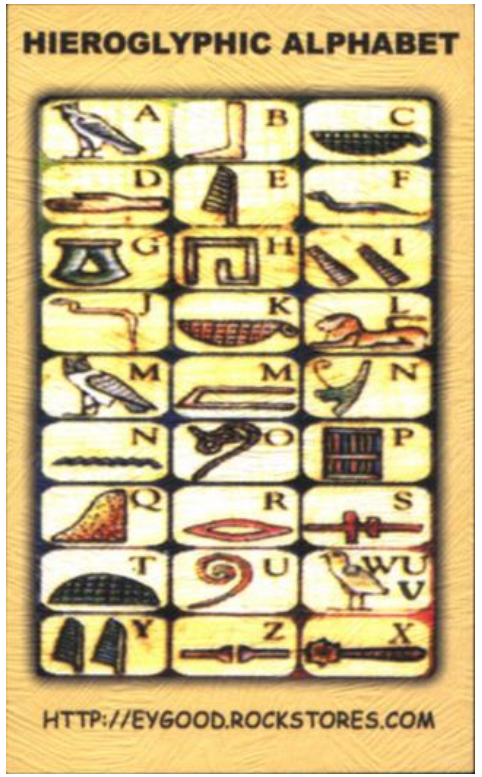
第一章 引言

- 什么是安全？
- 外国古代密码艺术
- 中国古代密码艺术
- 密码学基本概念
- 密码分析学
- 古典密码体制

外国古代密码艺术

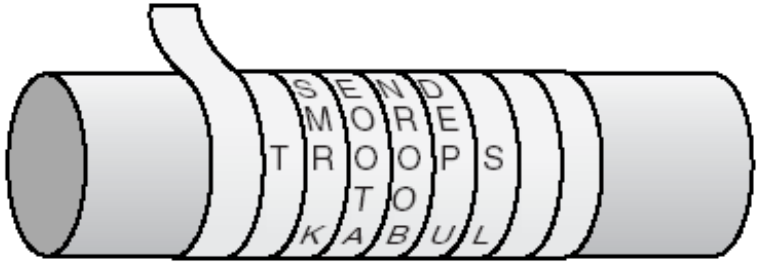
密码学的起源

- 象形文字的修改：密码学的第一个例子是对标准书写符号的修改，例如古埃及法老坟墓上的文字（3200-1100 B.C.），核心思想是代替(Substitution)



Scytale密码（天书）

500 B.C.，古斯巴达人使用的“天书”



棋盘密码

- 205-123 B.C.，古希腊人棋盘密码

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	IJ	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

HELLO → 2315313134

恺撒密码

- 50 B.C.，古罗马恺撒密码（移位密码或加法密码）

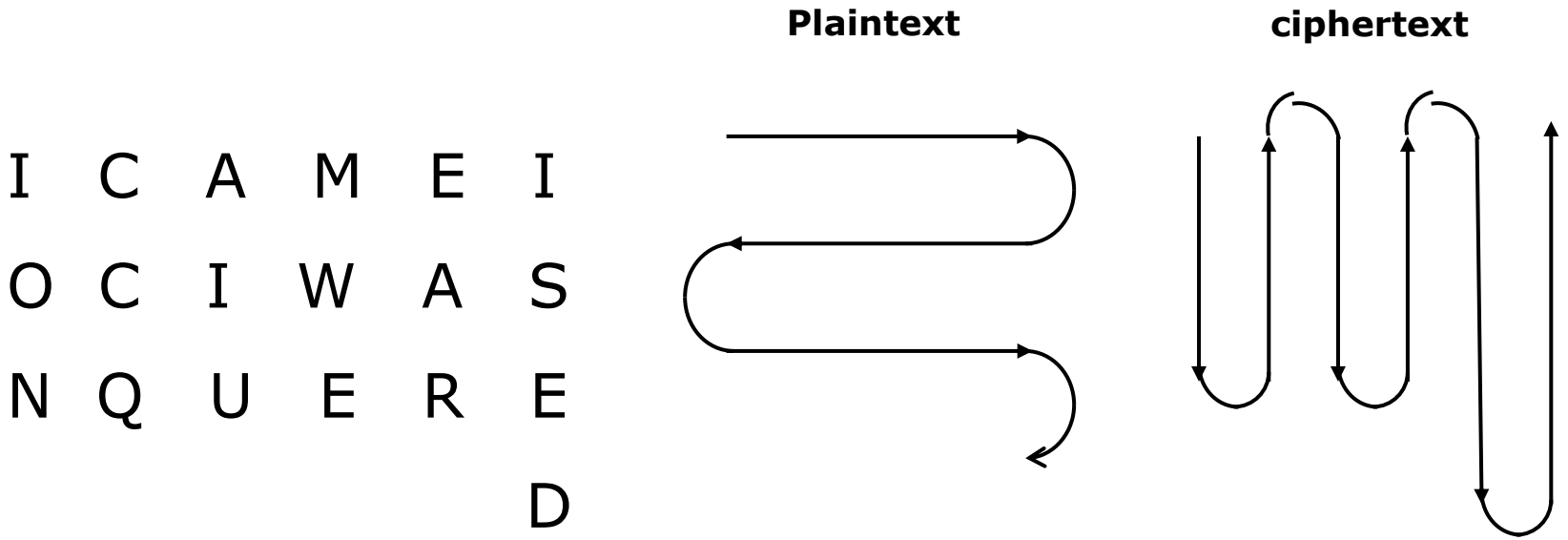
A	B	C	D	E	F	G	.....	X	Y	Z
D	E	F	G	H	I	J	.....	A	B	C

HELLO → KHOOR

1593年， 推广为Vigenère密码——分组加法密码

几何图形密码

- 以一种形式写下消息，以另一种形式读取消息
- 明文：**I came I saw I conquered**



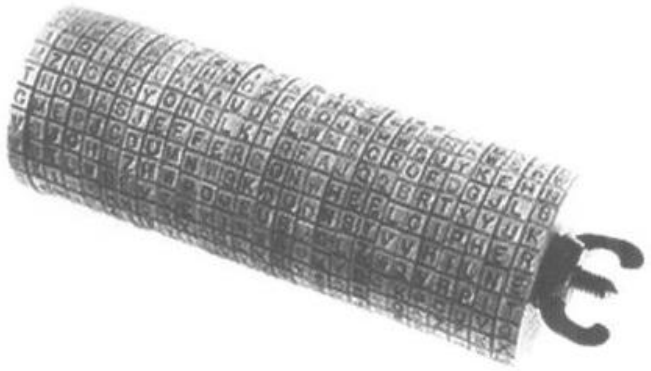
密文：**IONQC CAIUE WMEAR DESI**

杰弗逊密码

- 托马斯·杰弗逊（Thomas Jefferson，1743—1826），美国《独立宣言》的主要作者，并成为第三任美国总统（1801—1809）
- 杰弗逊对密码学深有研究。他在1795年发明了一种密码装置叫做杰弗逊圆盘（Jefferson disk）

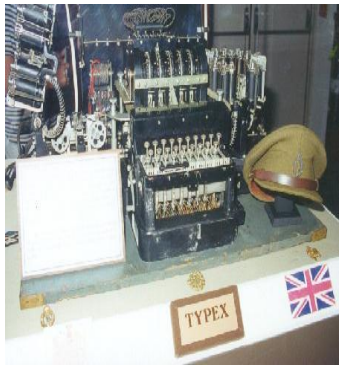
杰弗逊圆盘

- 这个装置有36片同样大小的木制转轮，套在一根铁杆上。每片转轮的圆周边缘上刻有乱序的26个英文字母
- 转动轮子使明文中的所有字母全排在一条直线上为止．这时圆柱体的其他25行字母也因这一行的固定而被固定了．任选这25行中的一行发出去即为密文.

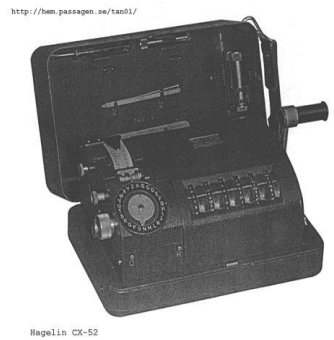


20世纪早期密码机


© Deutsches Museum


TYPEX

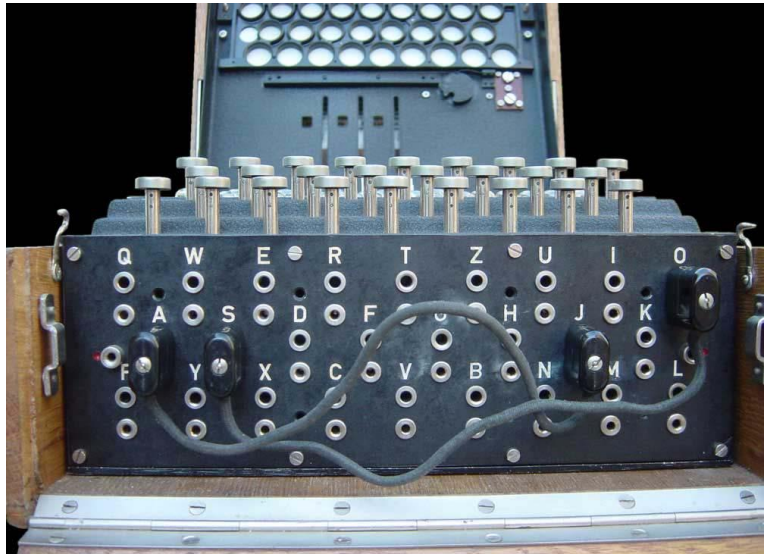

TUNNY


http://hem.passagen.se/tan01/
Hagelin CX-52

Enigma 密码机

- 12kg，28×34×15 cm

德Enigma密码机



破译Enigma

- 以往密码分析员是语言天才，而Enigma是机械装置，波兰总参二局密码处考虑：具有科学头脑的人破译它。
- 1929年1月，波兹南大学给波兰总参二局开列了一张系里最优秀的数学家名单，名单上有后来密码研究的“波兰三杰”。

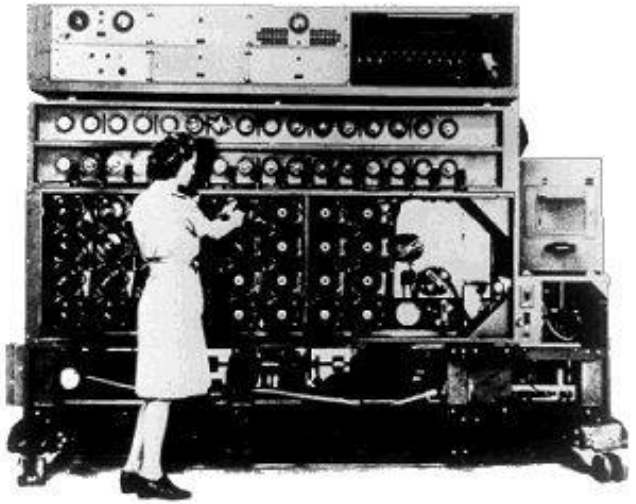
马里安·雷耶夫斯基

杰尔兹·罗佐基

亨里克·佐加尔斯基

破译Enigma

- 波兰三杰设计自动机械计算机 —“密码炸弹”（Bomba ）



破译Enigma

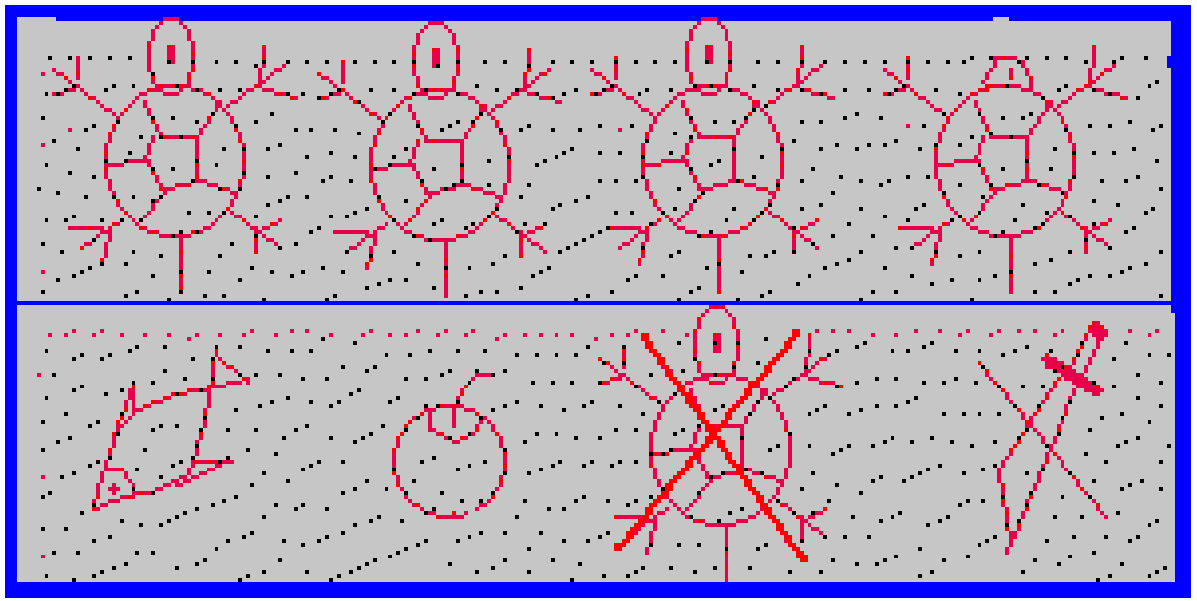
- 在1933年1月到1939年1月这六年，波兰方面一共破译了近十万条德方消息，最重要的有德国在包括苏台德地区兵力重新部署的情报
- 德国人1939年1月加强了密码机的安全性能，但是波兰人的实践表明：
  - Enigma决非坚不可破
  - 数学家在密码分析中的重要作用。
- 英国密码局（40局）以往都是精于文字的语言学家或作家，此后40局开始向牛津、剑桥招聘数学家和数学系学生

第一章 引言

- 什么是安全？
- 外国古代密码艺术
- 中国古代密码艺术
- 密码学基本概念
- 密码分析学
- 古典密码体制

一些例子

- 传说，古时候有一对夫妻，男的名叫李石匠，女的叫张小花。李石匠靠手艺赚钱，张小花在家纺纱织布。一年，李石匠参加修建石桥，因工程紧张，十一个月也没回家一次。张小花独自在家只有纺车做伴。一天石匠工地回来一个工友路过她家，她托这个工友给丈夫带去一封书信。



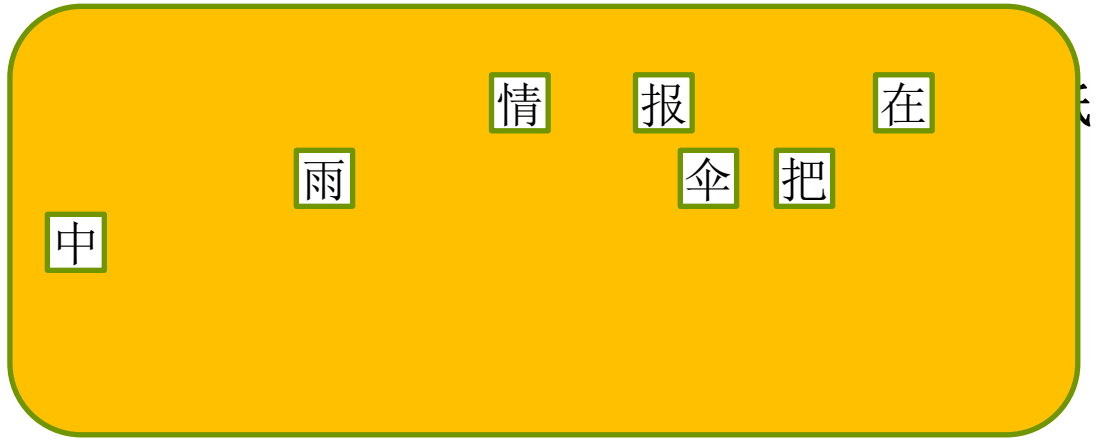
会意诗

叠痕法

- 先把信纸折叠几下（上下及左右），然后铺平信纸
- 将传递的信息按顺序一个个分开，写在折痕的交叉点上，每一个交叉点写一个字
- 在空白位置上填上公开的普通信文，普通信文与秘密信文的文字通顺地连贯在一起
- 为了防止被敌人察觉，使用这种密码需要在编公开信文上下些功夫。如果在秘密信文上再用些暗语式密码，那么敌人就更难看出破绽了。

漏格板加密法

例：密文：



明文：情报在雨伞把中。

阴符（〈六韬．龙韬．阴符〉）

- 武王问太公曰：‘引兵深入诸侯之地，三军猝有缓急，或利或害。吾将以近通远，从中应外，以给三军之用。为之奈何？’

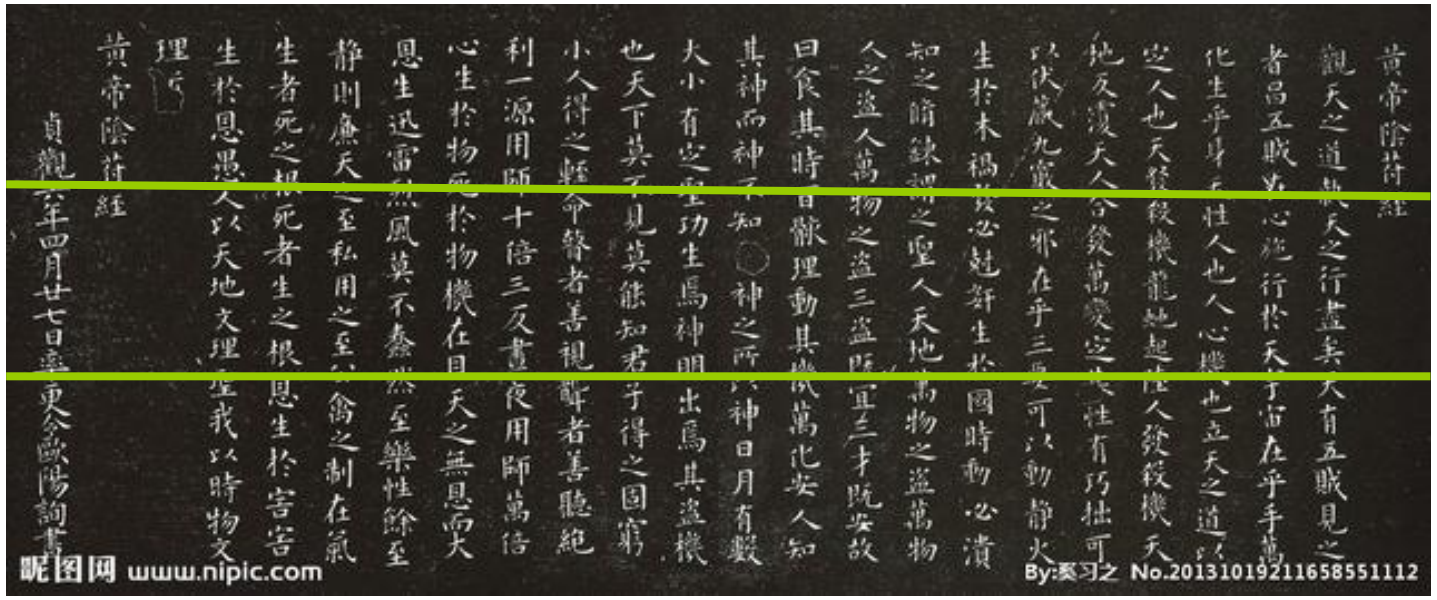
  太公曰：‘主与将，有阴符。凡八等：

  - 大胜克敌之符，长一尺；破军擒将之符，长九寸；
    降城得邑之符，长八寸；却敌报远之符，长七寸；
    警众坚守之符，长六寸；请粮益兵之符，长五寸；
    败军亡将之符，长四寸；失利亡士之符，长三寸。
- 八符者，主将秘闻，所以阴通言语，不泄中外相知之术。敌虽圣智，莫之通识。’

阴书（〈六韬．龙韬．阴书〉）

创造者：相传也是由姜子牙发明

用法：把一封竖写的秘密文书横截成3段，派出3个人各执一段，于不同时间、不同路线分别出发，先后送给收件者。收件者收齐了3段文件才能悉知秘密文书的全部内容。万一送件途中某一发送者被敌方截获，敌方也难以解读文书的全部内容。



中国古代军事密码（续）

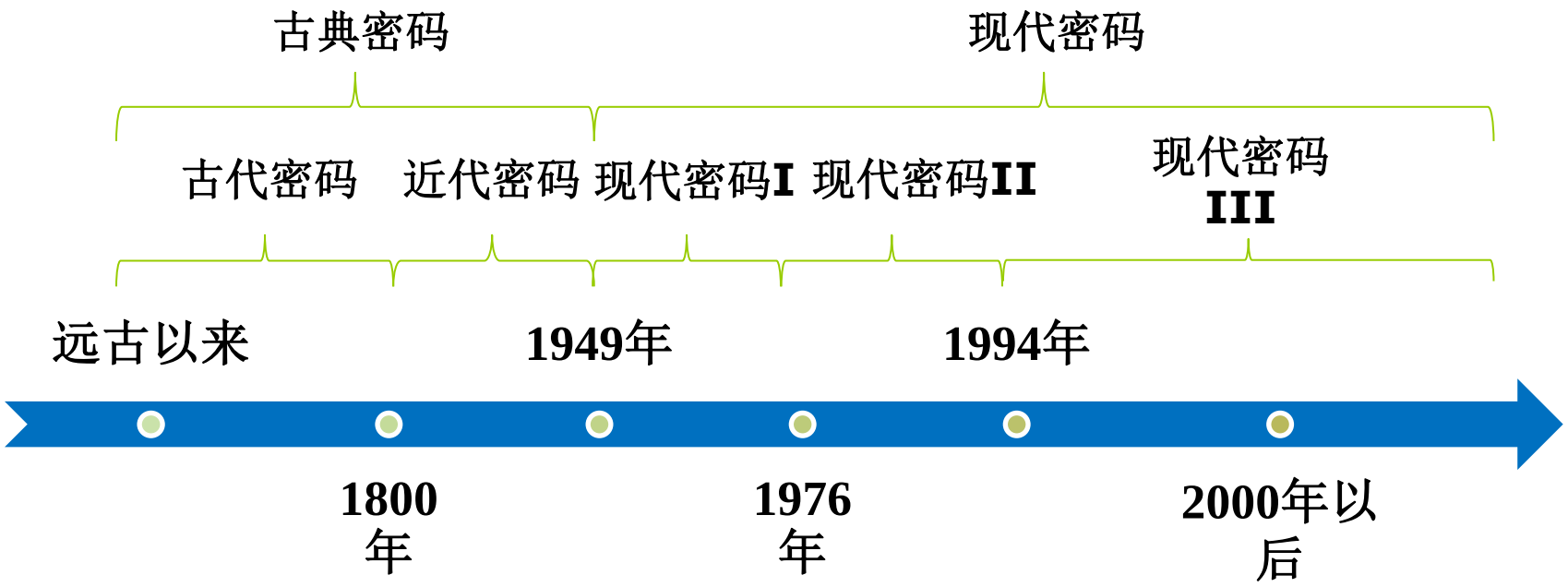
- 这套密码的使用方法是：
  - 约定一首**40**字的五言律诗
  - 保密，文字不得重复
- 假设双方以唐代王勃的《送杜少府之任蜀川》
  - 城阙辅三秦，风烟望五津。
  - 与君离别意，同是宦游人。
  - 海内存知己，天涯若比邻。
  - 无为在歧路，儿女共沾巾。

- 如果军队在战斗在粮食将尽，需要补充，前方将领就从密码本中查出“请粮料”的编码，是第九，而《送杜少府之任蜀川》中的第九字是“五”。于是请粮将领就将“五”字写到一件普通公文书牒之中，并在字上加盖印章。
- 指挥机关接到这件公文后，查出盖印章的“五”字，得知“五”字在临时约好的诗中列第九，再对照密码本上的顺序，就得知了前方的情报。

中国古代密码

- 加乱型：用有限元素(字母或数码)组成的一串 序列作为乱数，按规定的算法，与明信息序列相结合变成密信息。乱数序列可以有反复，也可以无反复。乱数序列一般是二元序列。它与明信息序列的结合方式有的采用模二加或逻辑同；有的采用模**N**加。如：
- 明码：　　中　　国　　人　　民　　……
- 　　**0022　0948　0086　3046　　……**
- 乱数：　**2901　4561　8265　7039　　……**
- 密文：　**2923　4409　8241　0075　　……**
- **C1(密)＝M1(明)＋K1(乱)　(mod　10)**
- **M1(明)＝C1(密)－K1(乱)　(mod　10)**

密码学发展时间轴


古典密码
现代密码
古代密码
近代密码
现代密码I
现代密码II
现代密码
III
远古以来
1949年
1994年
1800
年
1976
年
2000年以
后

古典密码——古代密码

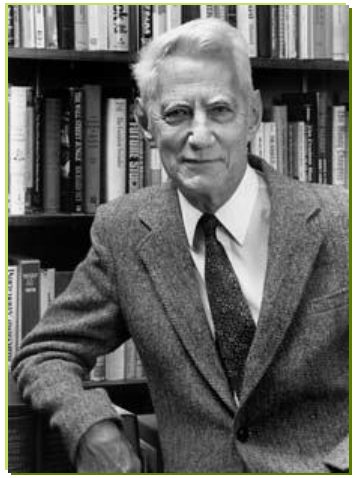
- 时间区域：从由人类以来到1800年
- 密码设计与分析被当作一门艺术
- 这一时期的密码学专家常常是凭直觉和信念来进行密码设计和分析，而不是靠推理证明
- 数据的保密基于加密算法的保密
- 密码工作者多为语言学家、猜谜高手等

古典密码——近代密码

- 时间区域：从**1800**到**1949**年
- 特点：
  - 密码机的迅速发展
  - 越来越多的数学家加入密码队伍
  - 出现一些密码算法和加密设备
  - 出现密码算法设计的基本手段(代替法 & 置换法)
- 保密性：
  - 数据的保密基于加密算法的保密

现代密码I阶段

时间跨度：**1949年-1976年**



1949年：

Shannon发表“The Communication Theory of Secret Systems”

- 定义理论安全性，提出扩散和混淆原则
- 奠定了密码学的理论基础
- 艺术→科学

- 保密性：
  - 数据的安全基于密钥而不是算法的保密

现代密码II阶段

时间跨度：**1976年-1994年**

- **1976年Diffie & Hellman的“New Directions in Cryptography”提出了公钥密码的概念**
- **1977年Rivest, Shamir & Adleman提出了RSA公钥算法**
- **1977年，DES成为了第一代公开的、完全说明细节的商业级密码标准**
- **90年代逐步出现椭圆曲线等其他公钥算法**

2015年图灵奖

公钥密码部分解决了对称密钥密码算法密钥共享和密钥管理困难的问题！

现代密码III阶段

- 时间区域：**1994**年至未来
  - **1994**年，**Shor**提出量子计算机模型下分解大整数和求解离散对数的多项式时间算法
  - **2000**年，**AES**正式取代**DES**成为了新的加密标准
  - **2006**年，第一届后量子密码学国际研讨会召开
  - **2017**年，**NIST**开始征集后量子密码标准

第一章 引言

- 什么是安全？
- 外国古代密码艺术
- 中国古代密码艺术
- 密码学基本概念
- 密码分析学
- 古典密码体制

什么是密码学？

- 密码学研究什么？
  - 如何使得某个数据自己能看懂，别人看不懂
  - 如何确保数据的正确来源
  - 如何保证通信实体的真实性
  - 如何确保数据在传输过程中没有被删改
  - 如何控制信息由指定的主体访问
- 功能如何实现
  - 算法
  - 协议

密码算法

- 基本概念
  - 明文**M**——要处理的数据 ------明文空间
  - 密文**C**——处理后的数据 ------密文空间
  - 密钥**k**——秘密参数 ------密钥空间
  - 加密函数：$C=E(k,M)$或$C=E_k(M)$ ------加密函数空间
  - 解密函数：$M=D(k,C)$或$M=D_k(C)$ ------解密函数空间

密码算法

- 密码算法需求：
  - 需求1：可逆——算法的使用者可以求得逆函数
  - 需求2：不可逆——敌手无法将密文恢复成明文
  - 秘密参数——密钥
- 密码算法实际上是一个带有秘密参数的函数。
  - 知道秘密参数，求逆非常容易
  - 不知道秘密参数，求逆在计算上是不可行的

单向函数 Oneway function

- **f(x)**是单向函数，如果它满足：
  - 已知**x**，计算**f(x)**是容易的
  - 已知**f(x)** ，计算**x**是困难的，即：在计算上是不可行的
- 例：
  - $f(x) = g^x \bmod p$， 其中**p**为大素数
  - **N = pq**， 求 **p**和**q**， 其中**p**、**q**为大素数
- 不存在函数已经证明是单向函数

单向函数 Oneway function

- 思考题：如果**f(x)**是单向函数，那么：
  - **g(x,r) = (f(x),r)**是单向函数吗？设**x**，**r**是等长的。
  - 如果**g(x,r)**不是单向函数，请说明理由；
  - 如果**g(x,r)**是单向函数，请说明理由，并思考单向函数到底能隐藏多少比特？

陷门单向函数 trapdoor oneway function

- **f(x)**是陷门单向函数，如果它满足：
  - 已知**x**，计算**f(x)**是容易的
  - 已知**f(x)**，计算**x**是困难的，即：在计算上是不可行的
  - 如果知道**trapdoor**，已知**f(x)**，计算**x**是容易的
- 例：
  - **RSA**加密算法

陷门单向函数 trapdoor oneway function

- 思考题：如果**f(x)**是陷门单向函数，那么：
  - **g(x,r) = (f(x),r)**是陷门单向函数吗？设**x**，**r**是等长的。
  - 如果**g(x,r)**不是陷门单向函数，请说明理由；
  - 如果**g(x,r)**是陷门单向函数，请说明理由，并思考陷门单向函数到底能隐藏多少比特？

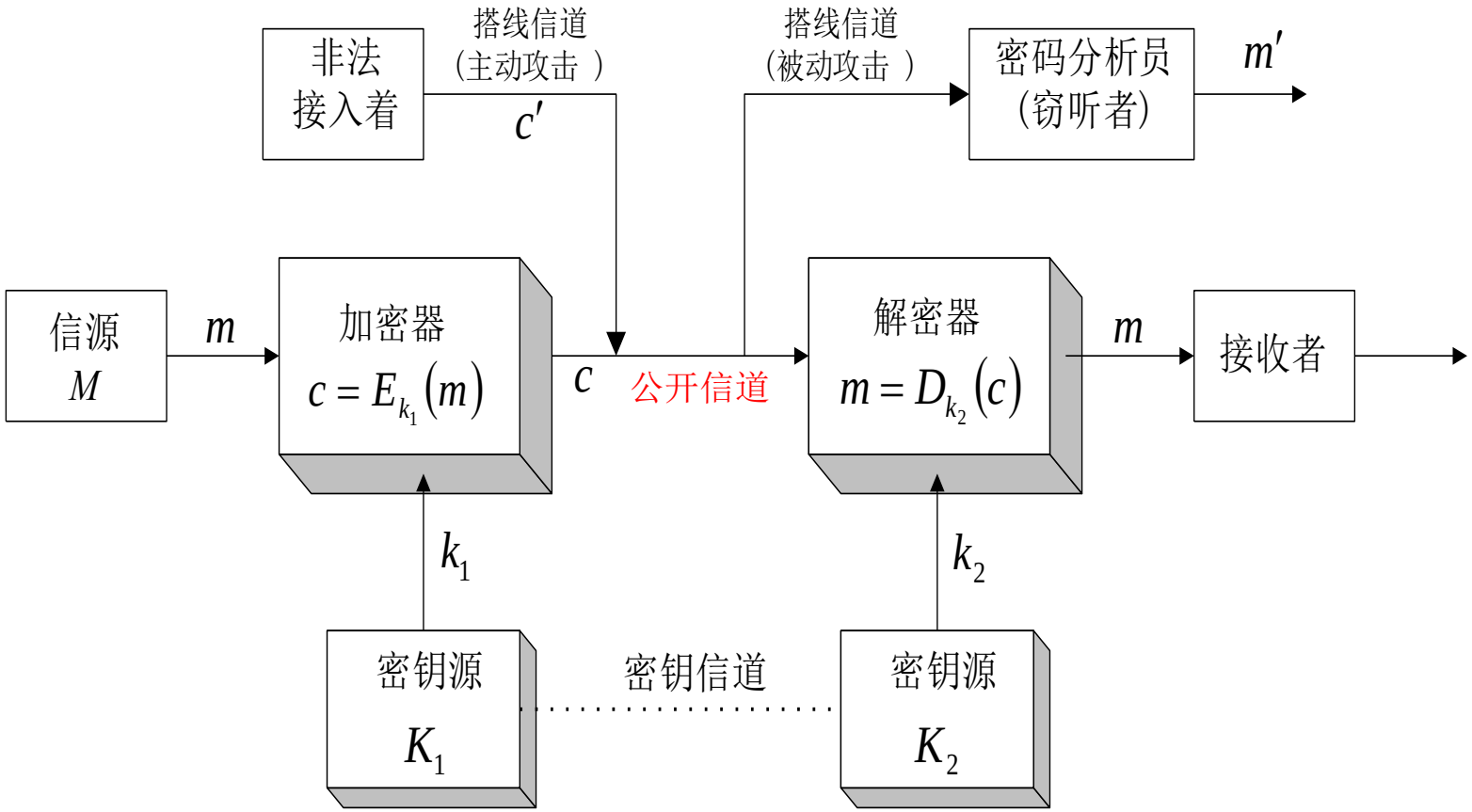
一个好的密码体制至少应满足的两个条件：

- (1) 在已知明文m和加密密钥k_1时，计算 $c = E_{k_1}(m)$ 容易，

  在已知密文c和解密密钥k_2时，计算$m = D_{k_2}(c)$容易；

- (2)在不知解密密钥k_2时，不可能由密文c恢复出明文m。

密码通信系统模型


非法
接入着
搭线信道
（主动攻击 ）
c'
搭线信道
（被动攻击 ）
密码分析员
（窃听者）
m'
信源
M
m
加密器
$c = E_{k_1}(m)$
c
公开信道
解密器
$m = D_{k_2}(c)$
m
接收者
k_1
k_2
密钥源
K_1
密钥信道
密钥源
K_2

密码算法的分类

- 按照功能分类
  - 加密算法：用于机密性解决方案
  - 杂凑函数：用于完整性解决方案
  - 数字签名：用于认证和不可否认性

密码算法的分类

- 按照密钥的使用方式不同分类

  - 对称密钥密码：加密密钥与解密密钥相同

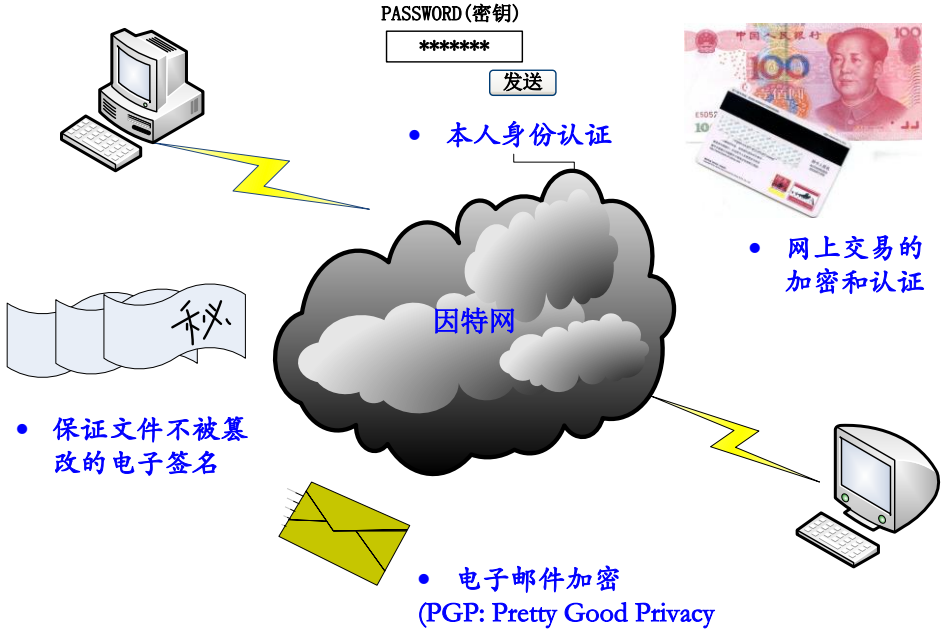
    如：分组密码，流密码

  - 非对称密钥密码体制：加密密钥与解密密钥不同

    如：公钥加密，数字签名

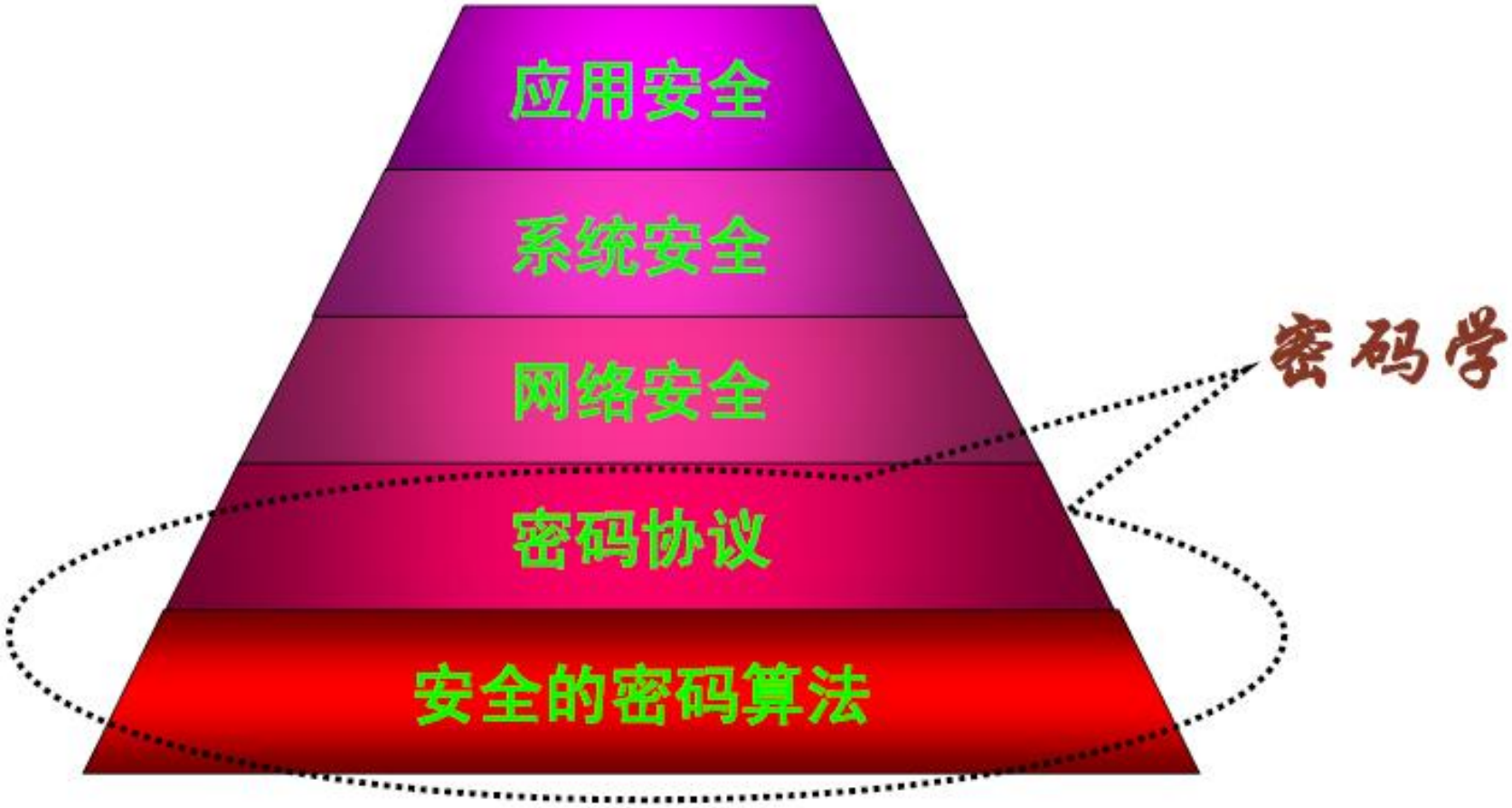
为什么需要密码学？

- **现代密码在社会中的广泛应用**



“密码技术”是保障信息安全的基本技术

密码学的地位和作用

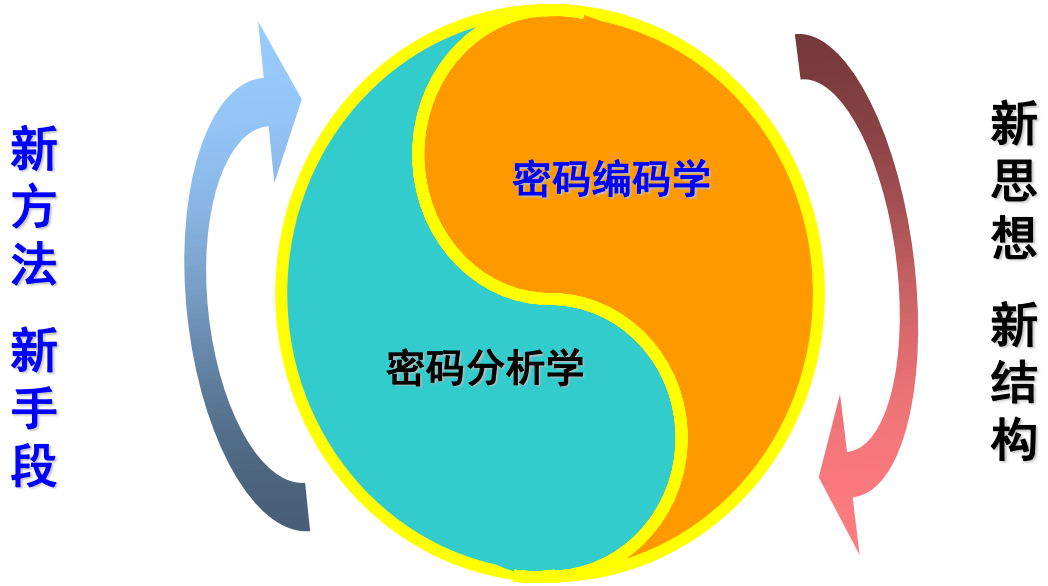


第一章 引言

- 什么是安全？
- 外国古代密码艺术
- 中国古代密码艺术
- 密码学基本概念
- 密码分析学
- 古典密码体制

密码学学科分支

- 两个分支形成既对立又统一的矛盾体



安全的概念

“如果把一封信锁在保险柜中，把保险柜藏起来，然后告诉你去看这封信，这并不是安全，而是隐藏；

相反，如果把一封信锁在保险柜中，然后把保险柜及其设计规范和许多同样的保险柜给你，以便你和世界上最好的开保险柜的专家能够研究锁的装置，而你还是无法打开保险柜去读这封信，这才是安全…”

-Bruce Schneier

密码分析学的前提

- **Kerckhoffs**假设：假定密码分析者和敌手知道所使用的密码系统。即密码体制的安全性仅依赖于对密钥的保密,而不应依赖于算法的保密
  - 假设敌手知道：
  - （1）所使用的加密算法
  - （2）知道明文的概率分布规律;
  - （3）知道密钥的概率分布规律;
  - （4）知道所有可能的破译方法
  - （5）敌手能够拿到加密装置，可以对其进行能量消耗分析等等

一切秘密皆蕴含在密钥中！

密码分析学的目标

- 目标：
  - 密文恢复
  - 密钥恢复

可破译的

可破译的：如果能够根据密文确定明文或密钥，或根据明文及对应的密文确定密钥；否则称为不可破译的。

其它的密码分析学目标

- 不可区分性：攻击者（敌手）在知道2个明文m0，m1的情况下，确定密文C对应的明文（ m0 or m1 ）

密码体制的攻击方法

密码分析者攻击密码体制的方法：

（1）穷举攻击：通过试遍所有的密钥来进行破译。

对抗：可增大密钥的数量。

（2）统计分析攻击：通过分析密文和明文的统计规律来破译。

对抗：设法使明文和密文的统计规律不一样。

（3）解密变换攻击：针对加密变换的数学基础，通过数学求解设法找到解密变换。

对抗：选用具有坚实的数学基础和足够复杂的加密算法。

密码体制的攻击（密码破译）

攻击强度

- 唯密文攻击（Ciphertext Olny Attack）
- 已知明文攻击（Known Plaintext Attack）
- 选择明文攻击（Chosen Plaintext Attack）
- 选择密文攻击（Chosen Ciphertext Attack）

这里一切的目的在于破译出密钥或者密文！

唯密文攻击

- 密码分析者仅知道一些密文。
- 最困难，一般是穷搜索，对截获密文用所有可能密钥去试
- 唯密文攻击敌手知道的信息量最少，最易抵抗
- 只要有足够的计算时间和存储容量，原则上可成功，但在实际上一种能保证安全要求的实用密码算法，都会设计得这一方法在实际上不可行
- 一般的敌手需要对密文进行统计测试分析，为此需要知道被加密的明文类型，英文文本，图象等。

已知明文攻击

- 密码分析者知道一些明文和相应的密文。
- 在很多情况下，敌手可能有更多的信息，也许能够截获一个或多个明文及其对应的密文，或消息中将出现某种明文格式，这时的攻击称为已知明文攻击，敌手也许能从已知的明文被变换成密文的方式得到密钥

选择明文攻击

- 密码分析者可以选择一些明文，并得到相应的密文。
- 如果攻击者能在加密系统中插入自己选择的明文消息，则通过该明文消息对应的密文有可能确定出密钥的结构
- 明文可以是精心选择的

选择密文攻击

- 密码分析者可以选择一些密文，并得到相应的明文。
- 攻击者利用解密算法，对自己所选的密文解密出相应的明文，有可能确定出密钥信息
- 选择的密文可以与要破解的密文相关

无条件安全与计算上安全

- 无条件安全的(不可破译的)：
  - 无论截获多少密文，都没有足够信息来唯一确定明文，则该密码是无条件安全的，即对算法的破译不比猜测有优势
- 计算上安全的：
  - 使用有效资源对一个密码系统进行分析而未能破译，则该密码是强的或计算上安全的

密码算法要满足的准则

密码算法只要满足以下两条准则之一就行：

（1） 破译密文的代价超过被加密信息的价值。

（2 ）破译密文所花的时间超过信息的有用期。

满足以上两个准则的密码算法在实际中是可用的。

第一章 引言

- 什么是安全？
- 外国古代密码艺术
- 中国古代密码艺术
- 密码学基本概念
- 密码分析学
- 古典密码体制

古典密码体制

古典密码的重要的两种构造方法，代替密码和置换密码

- 单表代替密码
- 多表代换密码

古典密码

- 古典密码的加密: 代换

字母	a	b	c	d	e	f	g	h	i	j	k	l	m
数字	0	1	2	3	4	5	6	7	8	9	10	11	12
字母	n	o	p	q	r	s	t	u	v	w	x	y	z
数字	13	14	15	16	17	18	19	20	21	22	23	24	25

表1-2 英文字母和十进制数字的对应关系

根据代换是对每个字母逐个进行还是对多个字母同时进行，古典密码又分为单表代换密码和多表代换密码。

古典密码的加密是将明文的每一字母代换为字母表中的另一字母，代换前首先将明文字母用等价的十进制数字代替，再以代替后的十进制数字进行运算，字母与十进制数字的对应关系如表 1-2 所示。

表 1-2　英文字母和十进制数的对应关系

字母	a	b	c	d	e	f	g	h	i	j	k	l	m
数字	0	1	2	3	4	5	6	7	8	9	10	11	12
字母	n	o	p	q	r	s	t	u	v	w	x	y	z
数字	13	14	15	16	17	18	19	20	21	22	23	24	25

根据代换是对每个字母逐个进行还是对多个字母同时进行，古典密码又分为单表代换密码和多表代换密码。

1.3.1 置换密码

在置换密码体制中，明文中的字或字母被重新排列，字或字母本身不变，但位置发生了改变，形成密文，又称为易位密码。

最简单的易位密码是采用报文倒置法，即将报文按字的顺序依次倒置，并截成固定长度的字母组，形成密文.

明文：never accept failure no matter how often it visits you

密文：uoys tisi vtin etfo wohr etta mone ulia ftpe ccar even

特点： 简单，缺点是不安全，很容易被识破。

1.3.2 单表代替密码

代替密码是把明文中的每一个字符替换成密文字母表中的另一个字符，并使用密钥*K*与之进行运算，得到密文.

接收者对密文进行逆运算就可以恢复出明文。

1.3.2 单表代替密码

单表代换密码又可以分为

- 加法密码
- 乘法密码
- 仿射密码
- 密钥短语代替密码

1.3.2 单表代替密码

1、加法密码

y=x+k（mod26)

明文：**x**

密文：**y**

密钥：**k**

解密：**x=y-k(mod26)**

Caesar密码就是一种加法密码

明文：**ATTACK START FROM TEN PM TONIGHT**

密文：**DW*W*DFN V*W*DUW IURP WHQ SP WRQLJKW**

1.3.2 单表代替密码

2、乘法密码

$$y=kx(mod26)$$

明文：**x**

密文：**y**

密钥：**k**

解密：$x=k^{-1}y(mod26)$

条件：**(k,26)=1**

1.3.2 单表代替密码

2、乘法密码，问题：

密钥空间有多少个元素？

1.3.2 单表代替密码

3、仿射密码

是乘法密码和加法密码的结合

$$y=ax+b(mod26)$$

明文：**x**

密文：**y**

密钥：**a,b**

解密：$x=a^{-1}(y-b)(mod26)$

条件：**(k,26)=1**

1.3.2 单表代替密码

3、仿射密码，问题：

密钥空间有多少个元素？

仿射密码算法

- 加密函数：$C=E(M)=aM+b \bmod 26$
- 密钥：a，b
- 解密函数：$M=D(C)=(C-b)a^{-1} \bmod 26$
- 关键在于计算a^{-1}：$a\ a^{-1}=1 \bmod 26$
- 方法：扩展的欧几里得算法
- 若$(m, n)=1$，则存在整数k_1，k_2使得

$$k_1 m + k_2 n = 1$$

这里k_1就是$m^{-1} \bmod n$，注意要将k_1变为正数

$-k_1 \bmod n=(n- k_1) \bmod n$

扩展的欧几里得算法

- 设a, b∈Z+, 则存在m, n∈Z, 使得
  gcd(a,b)=ma+nb.

$a=bq_1+r_1$ $\quad r_1=a-bq_1$

$b=r_1q_2+r_2$ $\quad r_2=b-r_1q_2$

$r_1=r_2q_3+r_3$, … $\quad r_3=r_1-r_2q_3$

… ……

$r_{n-2}=r_{n-1}q_n+r_n$ $\quad r_n=r_{n-2}-r_{n-1}q_n$

$gcd(a,b)=r_n=$

$r_{n-2}-r_{n-1}q_n$

=…… = ma+nb

- 求$17^{-1} \bmod 26$。
- $26 = 17 \times 1 + 9$
- $17 = 9 \times 1 + 8$
- $9 = 8 \times 1 + 1$
- $8 = 1 \times 8$

$1 = 9 - 8 \times 1$

$= 9 - (17 - 9 \times 1)$

$= 9 \times 2 - 17$

$= (26 - 17 \times 1) \times 2 - 17$

$= 26 \times 2 - 3 \times 17$

$-3 \bmod 26 = (26 - 3) \bmod 26 = 23$

因此$17^{-1} \bmod 26 = 23$

3. 仿射变换

仿射变换的加解密分别是：

$$c = E_{a,b}(m) \equiv am + b \pmod{26}$$

$$m = D_{a,b}(c) \equiv a^{-1}(c - b) \pmod{26}$$

其中 a、b 是密钥，为满足 $0 \le a,b \le 25$ 和 $\gcd(a,26) = 1$ 的整数。其中 $\gcd(a,26)$ 表示 a 和 26 的最大公因子，$\gcd(a,26) = 1$ 表示 a 和 26 是互素的，a^{-1} 表示 a 的逆元，即 $a^{-1} \cdot a \equiv 1 \bmod 26$。

【例 1-1】：设仿射变换的加解密分别是：

$$c = E_{7,21}(m) \equiv 7m + 21 \pmod{26}$$

$$m = D_{7,21}(c) \equiv 7^{-1}(c - 21) \pmod{26}$$

对 “security”加密，对 “vlxijh”解密。

$$
\begin{aligned}
s=18,\quad & 7\cdot 18+21\pmod{26}=17,\quad && s\Rightarrow r,\\
e=4,\quad & 7\cdot 4+21\pmod{26}=23,\quad && e\Rightarrow x,\\
c=2,\quad & 7\cdot 2+21\pmod{26}=9,\quad && c\Rightarrow j,\\
u=20,\quad & 7\cdot 20+21\pmod{26}=5,\quad && u\Rightarrow f,\\
r=17,\quad & 7\cdot 17+21\pmod{26}=10,\quad && r\Rightarrow k,\\
i=8,\quad & 7\cdot 8+21\pmod{26}=25,\quad && i\Rightarrow z,\\
t=19,\quad & 7\cdot 19+21\pmod{26}=24,\quad && t\Rightarrow y,\\
y=24,\quad & 7\cdot 24+21\pmod{26}=7,\quad && y\Rightarrow h.
\end{aligned}
$$

所以，“security”对应的密文是“rxjfkzyh”。

1.3.2 单表代替密码

4、密钥短语代替密码

这种密码选用一个英文短语或者单词串作为密钥，称为密钥字或密钥短语，

例如 HAPPY NEW YEAR，去掉其中的重复字母，得到一个无重复字母的字母串，即HAPYNEWR，把它依次写在明文字母表之下，而后再将字母表中未在字母串中出现过的字母依次写于此短语之后，就可以构造一个字母替换表

1.3.2 单表代替密码

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

当选择密钥短语代替密码和上述的密钥进行加密时，若明文为 **h e l l o**，则密文为**R N F F J**。不同的密钥字可以得到不同的替换表，对于明文为英文单词时，密钥短语密码最多可能 $26! = 4 \times 10^{26}$ 有个不同的替换表。

统计分析

字母	a	b	c	d	e	f	g
频率	0.0856	0.0139	0.0297	0.0678	0.1304	0.0289	0.0199
字母	h	i	j	k	l	m	n
频率	0.0528	0.0627	0.0013	0.0042	0.0339	0.0249	0.0707
字母	o	p	q	r	s	t	u
频率	0.0797	0.0199	0.0012	0.0677	0.0607	0.1045	0.0249
字母	v	w	x	y	z		
频率	0.0092	0.0149	0.0017	0.0199	0.0008		

Vige Vigenère密码

- 设m是某固定的正整数，定义 $P=C=K=(Z_{26})^m$，对一个密钥 $k=(k_1,k_2,\cdots;k_m)$，我们定义

$$e_k(x_1,x_2,\cdots;x_m)=(x_1+k_1,x_2+k_2,\cdots;x_m+k_m)$$

且 $d_k(y_1,y_2,\cdots;y_m)=(y_1-k_1,y_2-k_2,\cdots y_m-k_m)$

所有的运算都在 Z_{26}中。

注：此密码由法国密码学家Vigenère于1858年设计，1917年《Scientific American》声称此密码牢不可破，现在破译该密码“易如反掌”。

- 例　　设m＝6，且密钥字是CIPHER,这相应于密钥。假定明文串是　　**this cryptosystem is not secure**

首先将明文串转化为数字串，按6个一组分段，然后模26“加”上密钥字得:

19 7 8 18 2 17
2 8 15 7 4 17
21 15 23 25 6 8

18 19 4 12 8 18
2 8 15 7 4 17
21 1 19 19 12 9

20 17 4
2 8 15
22 25 19

24 15 19 14 18 24
2 8 15 7 4 17
0 23 8 21 22 15

13 14 19 18 4 2
2 8 15 7 4 17
15 22 8 25 8 19

相应的密文串将是:

VPXZGIAXIVWPUBTTMJPWIZITWZT

解密过程与加密过程类似,不同的只是进行模26减,而不是模26加。

1.4.2 多表代换密码

多表代换密码首先将明文M分为由n个字母构成的分组$M_1,M_2,\cdots,M_j$，对每个分组M_i的加密为：

$$C_i \equiv AM_i + B \pmod{N}, \quad i=1,2,\cdots,j$$

其中(A,B)是密钥，A是$n\times n$的可逆矩阵，满足$\gcd(|A|,N)=1$（$|A|$是行列式）。$B=(B_1,B_2,\cdots,B_n)^T, C=(C_1,C_2,\cdots,C_n)^T, M_i=(m_1,m_2,\cdots,m_n)^T$。对密文分组$C_i$的解密为：

$$M_i \equiv A^{-1}(C_i - B) \pmod{N}, \quad i=1,2,\cdots,j$$

【例 1-2】：设 $n=3, N=26$，

$$A=\begin{pmatrix}11 & 2 & 19\\ 5 & 23 & 25\\ 20 & 7 & 17\end{pmatrix}, B=\begin{pmatrix}0\\0\\0\end{pmatrix}$$

明文为“YOUR PIN NO IS FOUR ONE TWO SIX”。

将明文分成 3 个字母组成的分组“YOU RPI NNO ISF OUR ONE TWO SIX”，由表 1-2 得

$$M_1=\begin{pmatrix}24\\14\\20\end{pmatrix}, M_2=\begin{pmatrix}17\\15\\8\end{pmatrix}, M_3=\begin{pmatrix}13\\13\\14\end{pmatrix}, M_4=\begin{pmatrix}8\\18\\5\end{pmatrix},$$

$$M_5=\begin{pmatrix}14\\20\\17\end{pmatrix}, M_6=\begin{pmatrix}14\\13\\4\end{pmatrix}, M_7=\begin{pmatrix}19\\22\\14\end{pmatrix}, M_8=\begin{pmatrix}18\\8\\23\end{pmatrix}.$$

所以

$$C_1 = A\begin{pmatrix}24\\14\\20\end{pmatrix} = \begin{pmatrix}22\\6\\8\end{pmatrix}, C_2 = A\begin{pmatrix}17\\15\\8\end{pmatrix} = \begin{pmatrix}5\\6\\9\end{pmatrix}, C_3 = A\begin{pmatrix}13\\13\\14\end{pmatrix} = \begin{pmatrix}19\\12\\17\end{pmatrix}, C_4 = A\begin{pmatrix}8\\18\\5\end{pmatrix} = \begin{pmatrix}11\\7\\7\end{pmatrix},$$

$$C_5 = A\begin{pmatrix}14\\20\\17\end{pmatrix} = \begin{pmatrix}23\\19\\7\end{pmatrix}, C_6 = A\begin{pmatrix}14\\13\\4\end{pmatrix} = \begin{pmatrix}22\\1\\23\end{pmatrix}, C_7 = A\begin{pmatrix}19\\22\\14\end{pmatrix} = \begin{pmatrix}25\\15\\18\end{pmatrix}, C_8 = A\begin{pmatrix}18\\8\\23\end{pmatrix} = \begin{pmatrix}1\\17\\1\end{pmatrix}.$$

密文为 “WGI FGJ TMR LHH XTH WBX ZPS BRB”.

解密时，先求出

$$A^{-1}=\begin{pmatrix}11 & 2 & 19\\ 5 & 23 & 25\\ 20 & 7 & 17\end{pmatrix}^{-1}=\begin{pmatrix}10 & 23 & 7\\ 15 & 9 & 22\\ 5 & 9 & 21\end{pmatrix}$$

再求

$$M_1=A^{-1}\begin{pmatrix}22\\ 6\\ 8\end{pmatrix}=\begin{pmatrix}24\\ 14\\ 20\end{pmatrix},M_2=A^{-1}\begin{pmatrix}5\\ 6\\ 9\end{pmatrix}=\begin{pmatrix}17\\ 15\\ 8\end{pmatrix},M_3=A^{-1}\begin{pmatrix}19\\ 12\\ 17\end{pmatrix}=\begin{pmatrix}13\\ 13\\ 14\end{pmatrix},$$

$$M_4=A^{-1}\begin{pmatrix}11\\ 7\\ 7\end{pmatrix}=\begin{pmatrix}8\\ 18\\ 5\end{pmatrix},M_5=A^{-1}\begin{pmatrix}23\\ 19\\ 7\end{pmatrix}=\begin{pmatrix}14\\ 20\\ 17\end{pmatrix},M_6=A^{-1}\begin{pmatrix}22\\ 1\\ 23\end{pmatrix}=\begin{pmatrix}14\\ 13\\ 4\end{pmatrix},$$

$$M_7 = A^{-1}\begin{pmatrix}25\\15\\18\end{pmatrix} = \begin{pmatrix}19\\22\\14\end{pmatrix}, M_8 = A^{-1}\begin{pmatrix}1\\17\\1\end{pmatrix} = \begin{pmatrix}18\\8\\23\end{pmatrix}.$$

得明文为“YOU RPI NNO ISF OUR ONE TWO SIX”。

问题：

如果让大家来设计加密机制，基本思想是什么？

答案：

问题太复杂，不好回答

但是基本思想是：$f_1(f_2\bullet\bullet\bullet(f_n(x)))$

古典（经典）密码复合，就是乘积密码。

作业

1．设仿射变换的加密是：

$$E_{11,23}(m) \equiv 11m + 23 (\mathrm{mod}\, 26)$$

对明文“SECURITY”加密，并使用解密变换：

$$D_{11,23}(c) \equiv 11^{-1}(c - 23)\ (\mathrm{mod}\, 26)$$

验证你的加密结果。

2．给出保密通信系统的安全需求分析。