



信息安全概论

密码学基础

张伟哲 刘亚维



主要内容

2.1 密码学基础知识

2.2 古典替换密码

2.3 对称密钥密码

2.4 公开密钥密码

2.5 消息认证

2.6 密码学新进展

2.1 密码学基础知识

○ 为什么需要密码算法

- 信息的存储:存放在公开的地方
- 信息的交换:使用非隐秘介质
- 信息的传输:通过不安全信道

○ 解决数据的机密性、完整性、不可否认性以及身份识别等问题均需要以密码为基础

- 密码技术是保障信息安全的核心基础。

密码学的发展历史

- 第1阶段：1949年以前。
- 第2阶段：从1949年到1975年。
 - 标志：1949年Shannon发表的《保密系统的通信理论》一文。
- 第3阶段：1976年至今。
 - 标志：1976年Diffie和Hellman发表了《密码学新方向》一文。

第一阶段




- **1949**年以前的密码技术可以说是一种艺术，而不是一种科学，那时的密码专家是凭直觉和信念来进行密码设计和分析的，而不是靠推理证明。

第二阶段

- 1948年，**C. E. Shannon(1916~2002)**在贝尔系统技术杂志上发表论文《通信的数学理论》，创立了著名的新理论——信息论，标志着密码术到密码学的转变。
- 1949年**C. E. Shannon**发表的“保密系统的通信理论”一文为密码学奠定了坚实的理论基础，使密码学成为一门真正的科学。



第二阶段



- **Claude Shannon** was born on April 30, 1916 in the town of Gaylord, Michigan.
- By the 1980's, Shannon began having problems with his memory and he was later diagnosed with Alzheimer's disease.
- In his final years he was “good-natured as usual” and enjoyed daily visits with his wife, Betsy. Eventually his body failed and he passed away in February 2001.
- **A Mathematical Theory of Communication.** Bell Syst. Tech. J., 27:379-423, 1948
- **Communication Theory of Secrecy Systems.** Bell Syst. Tech. J., 28: 656-715, 1949

第三阶段



- 从**1976**年至今。
- 1976年Diffie和Hellman发表了“密码学的新方向(New Direction in Cryptography)”一文，提出了一种崭新的密码设计思想，导致了密码学的一场革命。
- IEEE Trans. Infor. Theory Vol.IT-22,p644-654,1976



密码学的两件大事

- 20世纪**70**年代中期，密码学界发生了两件跨时代的大事：
- **(1) Diffie和Hellman**发表的题为“密码学的新方向”文章，提出了“公钥密码”新体制，冲破了传统“单钥密码”体制的束缚。
 - 传统密码体制主要功能是信息的保密，双钥(公钥)密码体制不但赋予了通信的保密性，而且还提供了消息的认证性
 - 新的双钥密码体制无需事先交换秘密钥就可通过不安全信道安全地传递信息，大大简化了密钥分配的工作量。
 - 双钥密码体制适应了通信网的需要，为保密学技术应用于商业领域开辟了广阔的天地。

密码学的两件大事

- (2)美国国家标准局**NBS**于**1977**年公布实施美国数据加密标准**DES**，保密学史上第一次公开加密算法，并广泛应用于商用数据加密
- 这两件引人注目的大事揭开了保密学的神秘面纱，标志着保密学的理论与技术的划时代的革命性变革，为保密学的研究真正走向社会化作出了巨大贡献，同时也为保密学开辟了广泛的应用前景。
- 从此，掀起了现代密码学研究的高潮。

密码学的发展历史

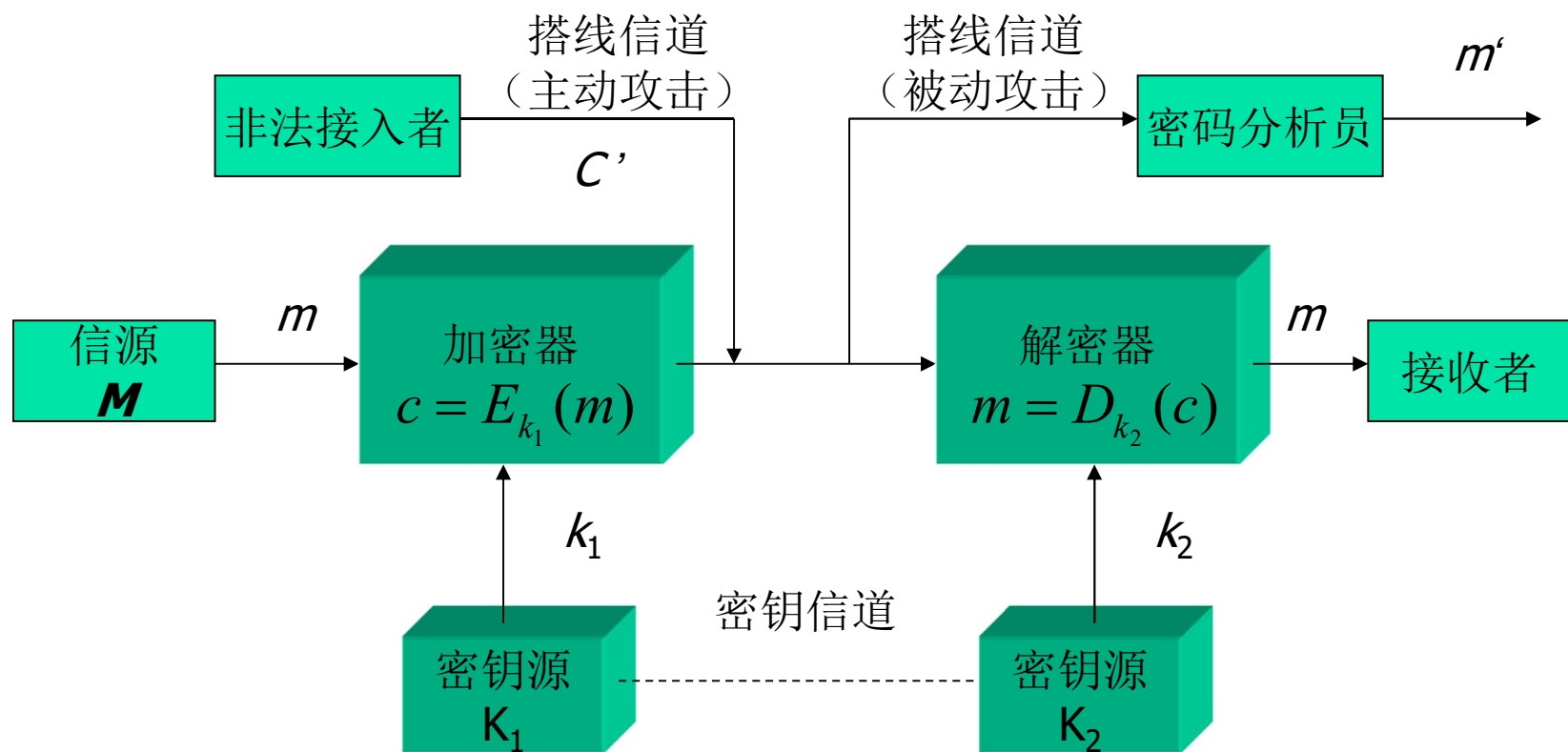


- 历史上的战争，特别是两次世界大战，对于保密学的理论与技术的发展起了巨大的推动作用。
- 在通信安全、保密、密码分析上的优势，被认为是赢得历史上许多主要军事冲突(包括二次世界大战)胜利的关键因素之一。

基本术语Basic Terminology

- 明文(plaintext) - 原文 (original message)
- 密文(ciphertext) - 加密后的消息 (coded message)
- 密码算法(cipher) -明文与密文转换的算法(algorithm)
- 密钥(key) -密码算法的输入, 实现明文与密文的转换
- 加密算法(encrypt) -明文转换为密文的算法
- 解密算法(decrypt) -密文转换为明文的算法
- 密码编码学(cryptography) -研究密码的原理及方法的理论
- 密码分析学(cryptanalysis)-研究破译密码获得信息及密钥的学科
- 密码学(cryptology) -密码编码学和密码分析学

密码体制



保密系统模型

密码算法公开性(known)

- Make it feasible for widespread use 便于广泛使用
- Low-cost chip implementations 低成本芯片实现
- Maintaining the secrecy of the key 密钥的管理
- 19世纪, Kerckhoff原则:
 - 系统的保密性不依赖于对加密体制或算法的保密, 而依赖于对密钥的保密。

密码体制

- 完整密码体制要包括如下五个要素
 - M是可能明文的有限集称为明文空间；
 - C是可能密文的有限集称为密文空间；
 - K是一切可能密钥构成的有限集称为密钥空间；
 - E为加密算法，对于任一密钥，都能够有效地计算；
 - D为解密算法，对于任一密钥，都能够有效地计算。
- 密码体系必须满足如下特性：
 - 加密算法($E_k: M \rightarrow C$)和解密算法($D_k: C \rightarrow M$)满足：
 - $D_k(E_k(x)) = x$, 这里 $x \in M$;
 - 破译者不能在有效的时间内破解出密钥k或明文x。

密码体制分类

- 密码体制有**2**大类：

- 单钥体制 (One-key system) :

- 加密密钥和解密密钥相同。

- 也称传统密码，对称密码。

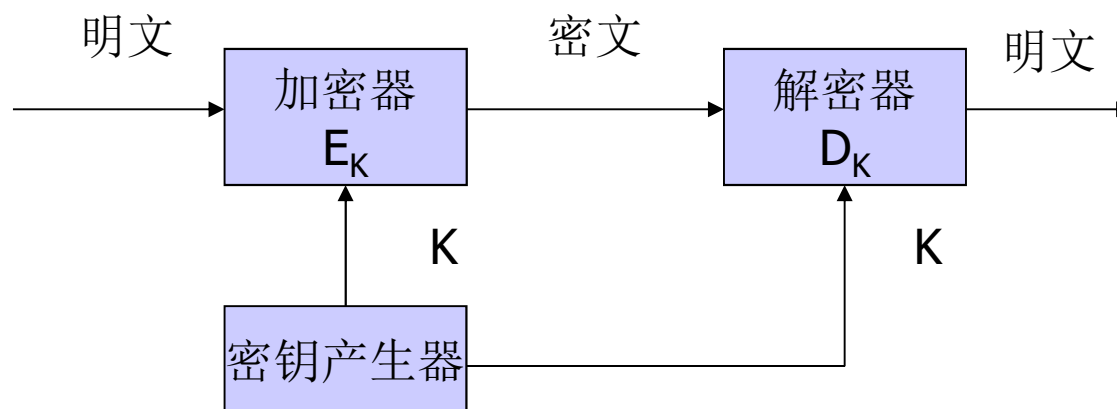
- 双钥体制 (Two key system) :

- 加密密钥和解密密钥不同。

- 也称公钥密码，非对称密码。

密码体制分类

单钥体制



密码体制分类 单钥体制

- 单钥体制主要研究问题：

- 密钥产生 (Key generation),
- 密钥管理 (Key management)。

- 分类：

- 流密码 (Stream cipher)
- 分组密码 (Block cipher)

- 单钥体制不仅可用于数据加密，也可用于消息的认证。



密码体制分类 双钥体制

双钥体制或公钥体制(Public key system) (Diffie和Hellman, 1976)

每个用户都有一对选定的密钥(公钥 k_1 ; 私钥 k_2), 公开的密钥 k_1 可以像电话号码一样进行注册公布。

公钥体制的主要特点

- 加密和解密能力分开
- 可以实现多个用户加密的消息只能由一个用户解读（用于公共网络中实现保密通信）
- 只能由一个用户加密消息而使多个用户可以解读（可用于认证系统中对消息进行数字签字）。
- 无需事先分配密钥。

密码编码学

Cryptography

- 研究内容

- 主要研究对信息进行编码，实现对信息的**隐蔽**。

- 特征

- 转换明文为密文的运算类型：代换与置换
- 所用的密钥数：单钥与双钥
- 处理明文的方法：分组密码与流密码

密码分析学

Cryptanalysis

- 目的：得到密钥，而不是仅仅得到单个密文对应的明文。
- 密码分析在外交、军事、公安、商业等方面都具有重要作用，也是研究历史、考古、古语言学和古乐理论的重要手段之一。

密码分析学

Cryptanalysis

- 密码设计和密码分析是共生的、又是互逆的，两者密切有关但追求的目标相反。两者解决问题的途径有很大差别
- 密码设计是利用数学来构造密码
- 密码分析除了依靠数学、工程背景、语言学等知识外，还要靠经验、统计、测试、眼力、直觉判断能力.....，有时还靠点运气。

基于密码分析的攻击

Cryptanalytic Attacks

- 惟密文攻击, **ciphertext only**
 - only know algorithm & ciphertext, is statistical, know or can identify plaintext
- 已知明文攻击, **known plaintext**
 - know/suspect plaintext & ciphertext
- 选择明文攻击, **chosen plaintext**
 - select plaintext and obtain ciphertext
- 选择密文攻击, **chosen ciphertext**
 - select ciphertext and obtain plaintext
- 选择文本攻击, **chosen text**
 - select plaintext or ciphertext to en/decrypt

两个概念

- 绝对安全， **unconditional security**
 - 无论花了多少时间，攻击者都无法将密文解密
 - 原因：攻击者所需要的信息不在密文里。
 - 一次一密
- 计算安全， **computational security**
 - 破译密码的代价超过密文信息的价值；
 - 破译密码的时间超出了密文信息的有效生命期。

密码分析方法--穷举破译法

- 对截收的密报依次用各种可解的密钥试译，直到得到有意义的明文；
- 或在不变密钥下，对所有可能的明文加密直到得到与截获密报一致为止，此法又称为完全试凑法(Complete trial-and-error Method)。
- 只要有足够多的计算时间和存储容量，原则上穷举法总是可以成功的。但实际中，任何一种能保障安全要求的实用密码都会设计得使这一方法在实际上是不可行的。

密码分析方法—分析法

- 确定性分析法

- 利用一个或几个已知量(比如, 已知密文或明文-密文对)用数学关系式表示出所求未知量(如密钥等)。已知量和未知量的关系视加密和解密算法而定, 寻求这种关系是确定性分析法的关键步骤。

- 统计分析法

- 利用明文的已知统计规律进行破译的方法。密码破译者对截收的密文进行统计分析, 总结出其间的统计规律, 并与明文的统计规律进行对照比较, 从中提取出明文和密文之间的对应或变换信息。

穷举攻击

Key Size (bits)	Number of Alternative Keys	Time required at 1 decryption/ μ s	Time required at 10^6 decryptions/ μ s
32	$2^{32} = 4.3 \times 10^9$	$2^{31} \mu\text{s} = 35.8 \text{ minutes}$	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	$2^{55} \mu\text{s} = 1142 \text{ years}$	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	$2^{127} \mu\text{s} = 5.4 \times 10^{24} \text{ years}$	$5.4 \times 10^{18} \text{ years}$
168	$2^{168} = 3.7 \times 10^{50}$	$2^{167} \mu\text{s} = 5.9 \times 10^{36} \text{ years}$	$5.9 \times 10^{30} \text{ years}$
26 characters (permutation)	$26! = 4 \times 10^{26}$	$2 \times 10^{26} \mu\text{s} = 6.4 \times 10^{12} \text{ years}$	$6.4 \times 10^6 \text{ years}$

非技术因素的攻击

- 社会工程

- 偷窃

- 收买

- 逼问

- ...

2.2 古典密码

- 古典密码体制采用代换法(**Substitution**)或换位法(**Transposition or Permutation**)
 - 把明文换成密文。用其他字母、数字或符号代替明文字母的方法称为代换法；将明文字母的正常次序打乱的方法称为换位法（或置换法）。
- 代换法包括单表代换体制和多表换体制
 - 其中单表代换体制又包括加法密码，乘法密码、仿射密码等。

加法密码



- 具体算法是将字母表的字母右移 k 个位置，并对字母表长度作模运算。
 - 每一个字母具有两个属性，本身代表的含义，可计算的位置序列值：
 - 加密函数： $E_k(m) = (m + k) \bmod q$;
 - 解密函数： $D_k(c) = (c - k) \bmod q$;

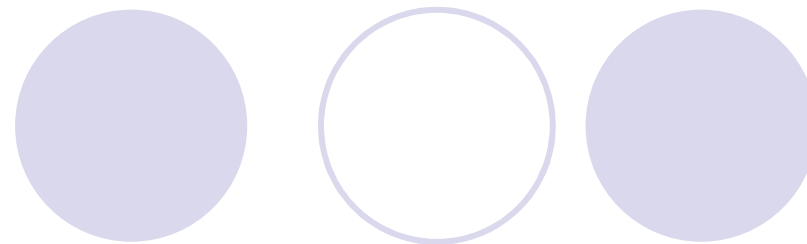
恺撒密码

Caesar Cipher

- 所知道的最早的代替密码
- **Julius Caesar**
- 首先用在军事通信中
- 用字母后的第三个字母代替

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

恺撒密码 - 加密



- 方式一：公式计算

- 明文编码：

如 $a=0$, $b=1$, ..., $z=25$, 则

明文 $P = p_1 p_2 \dots p_n$

(加密) 运算: $C_i = p_i + k \pmod{26}$, $i = 1, 2, \dots, n$

恺撒密码-加密

- 方式二：查表（例**k=3**）

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

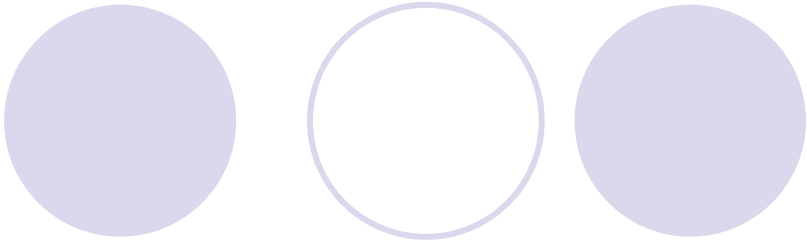
恺撒密码 - 解密

- 方式一：公式计算

- 密文 $\mathbf{C} = \mathbf{c}_1\mathbf{c}_2\cdots\mathbf{c}_n$

（加密）运算： $\mathbf{P}_i = \mathbf{c}_i - \mathbf{k} \pmod{26}, i=1,2,\dots,n$

恺撒密码-解密



- 方式二：查表（例**k=3**）

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

恺撒密码

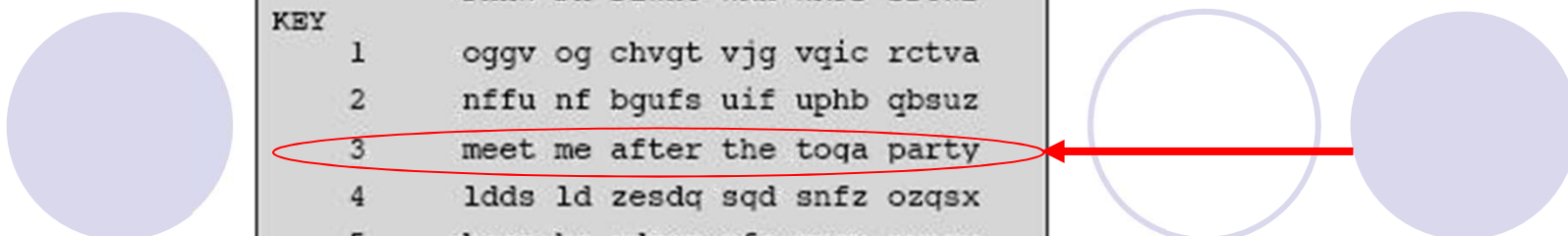
$$c = E(p) = (p + k) \bmod (26)$$

$$p = D(c) = (c - k) \bmod (26)$$

恺撒密码的密码分析

- 攻击方法：穷举攻击

- 已知加密和解密算法
- 共有密钥**25**个
- 所破译的明文其意义易于识别
- 如：破译密文 "GCUA VQ DTGCM"
 - dzrx sn aqdzj (k=3)
 - easy to break (k=2)



KEY		PHHW	PH	DIWHU	WKH	WRJD	SDUWB
1	oggv	og	chvgt	vjg	vqic	rctva	
2	nffu	nf	bgufs	uif	uphb	qbsuz	
3	meet	me	after	the	toqa	party	
4	ldds	ld	zesdq	sqd	snfz	ozqsx	
5	kccr	kc	ydrp	rfe	rmey	nyprw	
6	jbbq	jb	xcqbo	qeb	qldx	mxogv	
7	iaap	ia	wbpan	pda	pkcw	lwnpu	
8	hzzo	hz	vaozm	ocz	objv	kvmot	
9	qyyn	qy	uznyl	nby	niau	julns	
10	fxxm	fx	tymxk	max	mhzt	itkmr	
11	ewwl	ew	sxlwj	lzw	lgys	hsjlg	
12	dvvk	dv	rwkvi	kyv	kfxr	grikp	
13	cuuj	cu	qvjuh	jxu	jewq	fqhjo	
14	btti	bt	putq	iwt	idvp	epqin	
15	assh	as	othsf	hvs	hcuo	dofhm	
16	zrrg	zr	nsgre	gur	gbtn	cnegl	
17	yqqf	yq	mrfqd	ftq	fasm	bmdfk	
18	xppe	xp	lqepc	esp	ezrl	alcej	
19	wood	wo	kpdob	dro	dyqk	zkbdi	
20	vnnc	vn	jocna	cqn	cxpj	yjach	
21	ummb	um	inbmz	bpm	bwoi	xizbg	
22	tlla	tl	hmaly	aol	avnh	whyaf	
23	skkz	sk	qlzkx	znk	zumq	vqxze	
24	rjyy	rj	fkyjw	ymj	ytlf	ufwyd	
25	qiix	qi	ejxiv	xli	xske	tevxc	

Figure 2.3 Brute-Force Cryptanalysis of Caesar Cipher

乘数密码

- 乘数密码

- 将明文字母串逐位乘以密钥 k 并进行模运算。
- 数学表达式: $E_k(m) = k * m \bmod q, \gcd(k, q) = 1$ 。
 - $\gcd(k, q) = 1$ 表示 k 与 q 的最大公因子为1。
- 算法描述:
 - $M = C = Z/(26)$, 明文空间和密文空间同为英文字母表空间, 包含26个元素; $q = 26$;
 - $K = \{k \in \text{整数集} \mid 0 < k < 26, \gcd(k, 26) = 1\}$, 密钥为大于0小于26, 与26互素的正整数;
 - $E_k(m) = k m \bmod q$ 。
 - $D_k^{-1}(c) = k^{-1} c \bmod q$, 其中 k^{-1} 为 k 在模 q 下的乘法逆元。

密钥取值与乘法逆元

- 乘数密码的密钥 k 与26互素时，加密变换才是一一映射的，
 - k 的选择有11种：3、5、7、9、11、15、17、19、21、23、25。 k 取1时没有意义。
- k^{-1} 为 k 在模 q 下的乘法逆元，
 - 其定义为 $k^{-1} * k \bmod q = 1$ ，
 - 可采用扩展的欧几里德算法。欧几里德算法又称辗转相除法，用于计算两个整数 a 和 b 的最大公约数。

乘法密码举例

- 密钥 $k=5$ ，对hello进行加密
 - hello所对应的数字[8,5,12,12 15];
 - 加密后的数字为[14 , 25,8,8, 23];
 - 对应的密文消息就是nyhhw
- 解密密钥即 K 的逆元，为21

仿射密码

- 仿射密码

- 可以看作是移位密码和乘数密码的结合。

- 密码体制描述如下：

- $M=C=\mathbb{Z}/(26)$; $q=26$;

- $K=\{k_1, k_2 \in \mathbb{Z} \mid 0 < k_1, k_2 < 26, \gcd(k_1, 26)=1\}$;

- $E_k(m) = (k_1 m + k_2) \bmod q$;

- $D_k(c) = k_1^{-1}(c - k_2) \bmod q$, 其中 k_1^{-1} 为 k_1 在模 q 下的乘法逆元。

- 密钥情况, k_1 和 k_2 ?

仿射密码事例

○ 设 $k = (5, 3)$ ，注意到 $5^{-1} \bmod 26 = 21$ ，

○ 加密函数：

● $E_k(x) = 5x + 3 \pmod{26}$ ，

○ 解密函数：

● $D_k(y) = 21(y - 3) \bmod 26 = 21y - 11 \pmod{26}$ 。

○ 加密明文 “yes” 的加密与解密过程如下：

$$\begin{array}{c} E_k \left\{ \begin{array}{c} y \\ e \\ s \end{array} \right\} = 5 \times \left\{ \begin{array}{c} 24 \\ 4 \\ 18 \end{array} \right\} + \left\{ \begin{array}{c} 3 \\ 3 \\ 3 \end{array} \right\} = \left\{ \begin{array}{c} 19 \\ 23 \\ 15 \end{array} \right\} = \left\{ \begin{array}{c} t \\ x \\ p \end{array} \right\} \quad 21 \times \left\{ \begin{array}{c} 19 \\ 23 \\ 15 \end{array} \right\} - \left\{ \begin{array}{c} 11 \\ 11 \\ 11 \end{array} \right\} = \left\{ \begin{array}{c} 24 \\ 4 \\ 18 \end{array} \right\} = \left\{ \begin{array}{c} y \\ e \\ s \end{array} \right\} \\ \leftarrow \text{Mod } 26 \rightarrow \quad \leftarrow \text{Mod } 26 \rightarrow \\ \leftarrow \text{加密过程} \rightarrow \quad \leftarrow \text{解密过程} \rightarrow \end{array}$$

单表代替密码



- 不是简单有序地字母移位
- 每个明文字母映射到一个不同的随机密文字母
- 密钥数目： 26！

单表代替密码分析

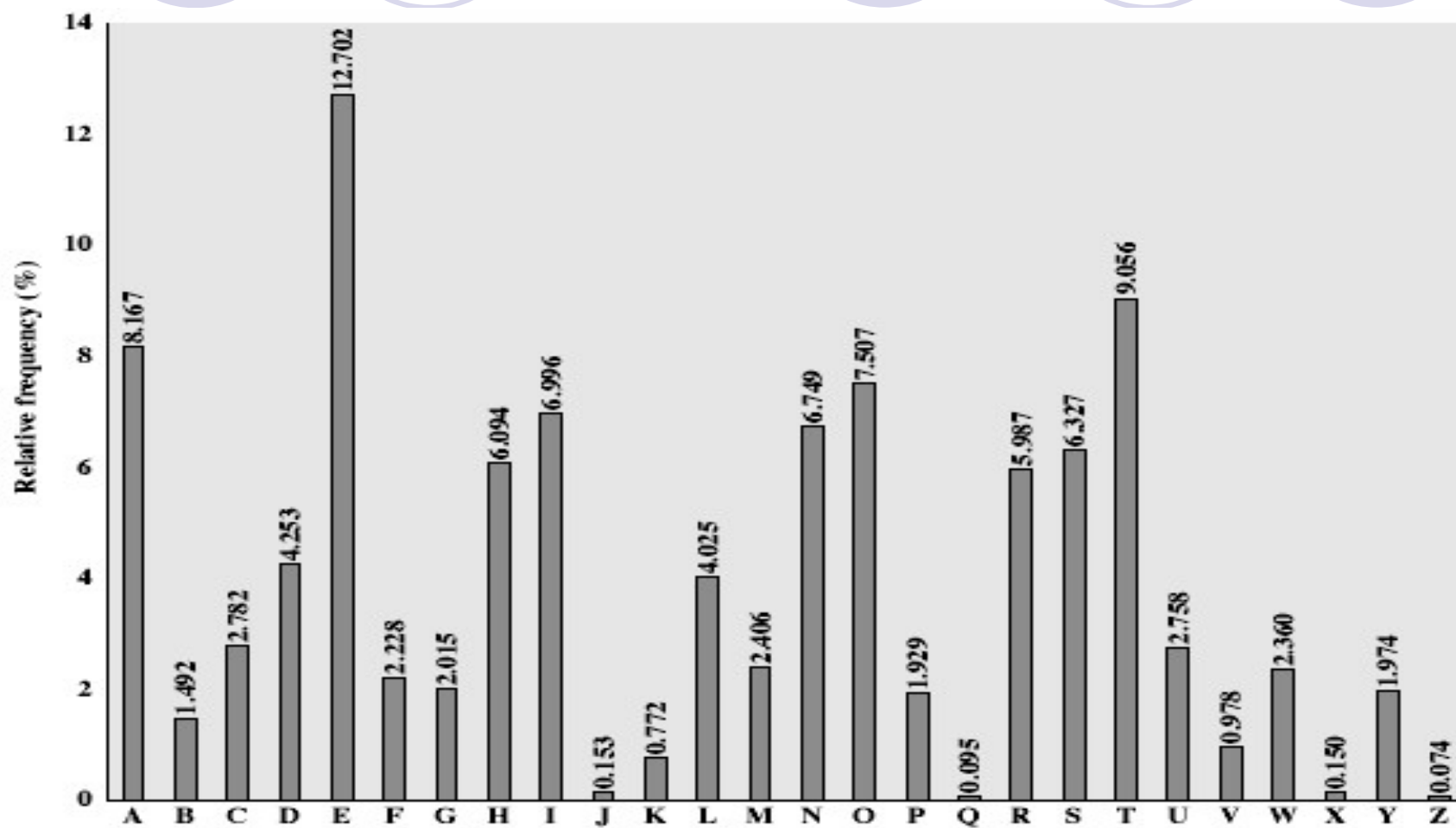
- 密钥空间: $26! > 4 \times 10^{26}$
- 貌似安全，实则不然
- 单表代替密码 容易被攻破，携带了语言的统计学特性。

语言的冗余与密码分析



- 人类的语言是有冗余的
- 字母的使用频率是不同的
- 在英语中**E**使用的频率最高
- 有些字母使用较少
- 单字母、双字母、三字母组合统计

英语字母使用频率



Playfair密码



- 单表代换缺陷是：密文带有原始字母使用频率的一些统计学特征。
- 对策：每个字母提供多种代换。
- **Playfair**密码是一个多表代替密码；
- Charles Wheatstone 于1854年发明, 用其朋友Baron Playfair 命名。
- 广泛用于第一次及二次世界大战

Playfair密钥矩阵

- 5 X 5
- 填写密钥单词
- 用其他字母填写剩下的空缺
- I = J

M	O	N	A	R
C	H	Y	B	D
E	F	G	I/J	K
L	P	Q	S	T
U	V	W	X	Z

Playfair密码的加/解密步骤

- 加密

- 明文分组（填充）：**2**个字母 / 组
- 同行字母对加密：循环向右，**ei**→**FK**
- 同列字母对加密：循环向下，**cu**→**EM**，**xi**→**AS**
- 其它字母对加密：矩形对角线字母，且按行排序，**hs**→**BP**，**es**→**IL**（或**JL**）

- 解密

- 加密的逆向操作

Playfair Key Matrix 密钥矩阵

M	O	N	A	R
C	H	Y	B	D
E	F	G	I/J	K
L	P	Q	S	T
U	V	W	X	Z

Ar → RM 同行取右边

mü → CM 同列取下边

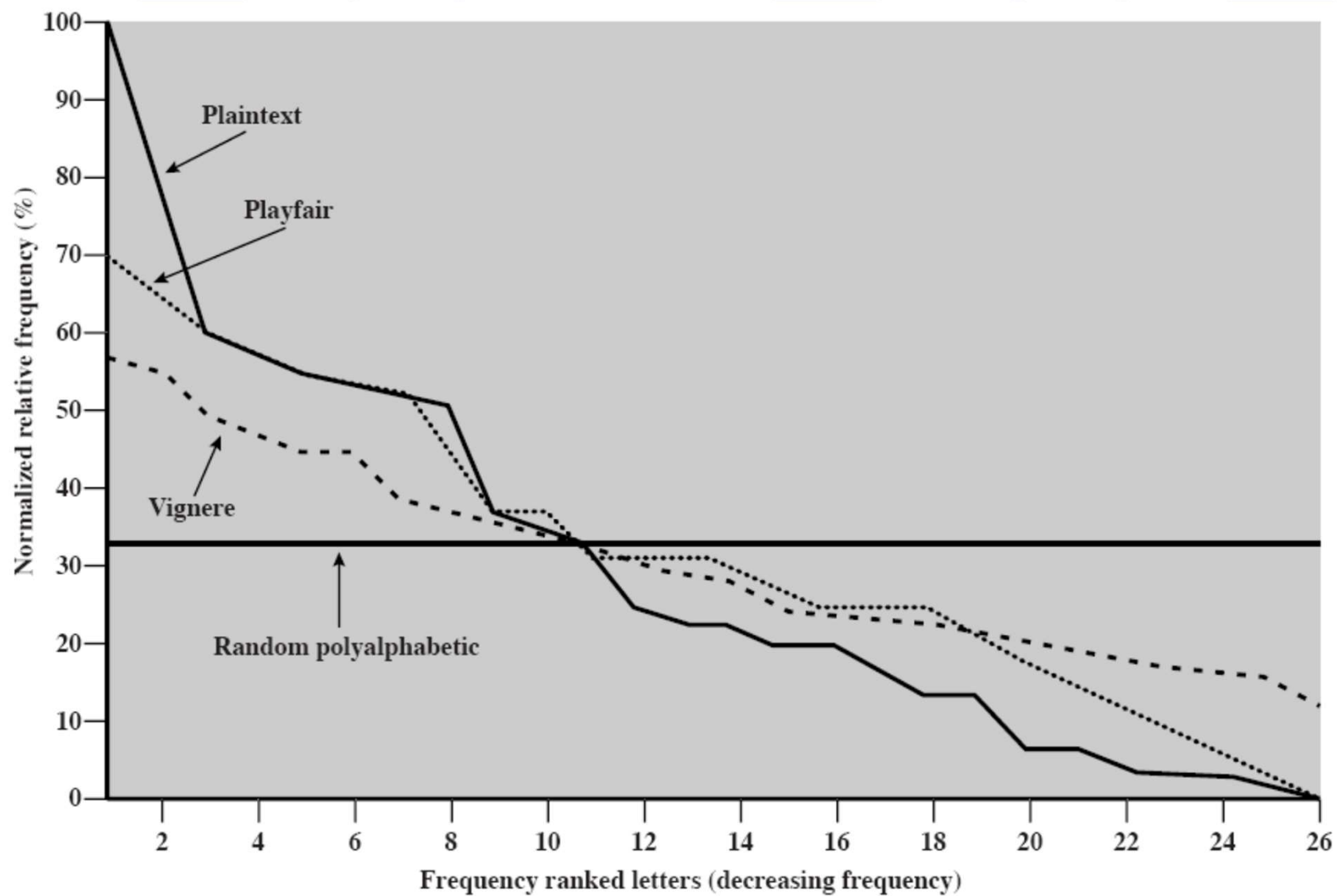
hs → BP

其它取交叉

ea → IM or JM

Playfair密码安全性分析

- 明、密文字母不是一一对应关系
- 安全性优于单表代替密码
- 在**WW1**中使用多年
- 虽然明文中文母的统计规律在密文中得到了降低，但密文中仍含有明文的部分结构信息
- 给定几百个字母，即可被攻破



字母出现的相对频率

希尔(Hill)密码

- 1929年由数学家Lester Hill发明
- 是多表代换密码
- 加密方法是由 m 个线性方程决定的。

Hill密码的加/解密过程

加密:

- 明文分组并编码
- $C \equiv KP \pmod{26}$, 其中, **K**为密钥矩阵, **P**、**C**分别为明、密文分组

解密:

- 密文分组并编码
- $P \equiv K^{-1}C \pmod{26}$

对密钥矩阵**K**的要求: 在mod 26下可逆.

Hill密码的例子

加密:

$$\text{密钥矩阵 } \mathbf{K} = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 9 \end{pmatrix}$$

$$\mathbf{K}^{-1} = \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix}$$

明文分组 $\mathbf{P} = \text{“mor”}$

$$\text{明文编码 } \mathbf{P} = \begin{pmatrix} m \\ o \\ r \end{pmatrix} = \begin{pmatrix} 12 \\ 14 \\ 17 \end{pmatrix}$$

$$\text{加密 } \mathbf{C} \equiv \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \begin{pmatrix} 12 \\ 14 \\ 17 \end{pmatrix} \equiv \begin{pmatrix} 527 \\ 651 \\ 375 \end{pmatrix} \equiv \begin{pmatrix} 7 \\ 3 \\ 11 \end{pmatrix} \pmod{26}$$

$$\mathbf{C} = \begin{pmatrix} H \\ D \\ L \end{pmatrix}, \text{ 即 } \mathbf{C} = \text{“HDL”}$$

Hill密码的例子

解密:

$$\text{密钥矩阵 } \mathbf{K} = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 9 \end{pmatrix}$$

$$\mathbf{K}^{-1} = \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix}$$

$$\mathbf{C} = \text{“HDL”} \quad \mathbf{C} = \begin{pmatrix} H \\ D \\ L \end{pmatrix} = \begin{pmatrix} 7 \\ 3 \\ 11 \end{pmatrix}$$

$$\text{解密 } \mathbf{P} \equiv \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} \begin{pmatrix} 7 \\ 3 \\ 11 \end{pmatrix} \equiv \begin{pmatrix} 220 \\ 222 \\ 355 \end{pmatrix} \equiv \begin{pmatrix} 12 \\ 14 \\ 17 \end{pmatrix} \bmod 26$$

$$\text{明文 } \mathbf{P} = \begin{pmatrix} 12 \\ 14 \\ 17 \end{pmatrix} = \begin{pmatrix} m \\ o \\ r \end{pmatrix}$$

明文 $\mathbf{P} = \text{“mor”}$

Hill密码的特点

- 明、密文字母不是一一对应关系
- 连续 m 个明文替换成 m 个密文
- 字母的统计规律进一步降低

多表代换密码

Polyalphabetic Ciphers

- 基于单表代换：在明文消息中采用不同的单表代换。
- 安全性提高
- 使得字母的频率分布更加平坦
- 例子：
 - **Vigenère**（维吉利亚）密码（1858）
 - **Vernam**（唯尔南）密码（1918）

一、Vigenère（维吉利亚）密码

加密:

- 方式一：数学公式计算

- 设明文 $P = p_1p_2\dots p_n$ ，密钥 $k = k_1k_2\dots k_n$ ，密文 $C = c_1c_2\dots c_n$

- 加密： $c_i = p_i + k_i \pmod{26}$, $i = 1, 2, \dots, n$;

- 说明：若明文长度大于 n ，则 K 重复使用。



一、Vigenère（维吉利亚）密码

● 方式二：查表法

Table 2.3 The Modern Vigenère Tableau

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

一、Vigenère（维吉利亚）密码

解密：

- 方法一：数学公式计算

- $p_i = c_i - k_i \pmod{26}, i = 1, 2, \dots, n;$

- 方法二：查表

Vigenère密码例子

- 加密过程:

○ P= “encode and decode”, k= “mykey”

字母序号		e	n	c	o	d	e	a	n	d	d	e	c	o	d	e
明文编码	P=	4	13	2	14	3	4	0	13	3	3	4	2	14	3	4
密钥编码	k=	12	24	10	4	24	12	24	10	4	24	12	24	10	4	24
加密	C=	16	37	12	18	27	16	24	23	7	27	16	26	24	7	28
模运算			11			1					1		0			2
密文解码	C=	Q	L	M	S	B	Q	Y	X	H	B	Q	A	Y	H	B

Vigenère密码例子

- 解密过程:

○ $C = \text{"QLMSBQYXHBQAYHB"} , k = \text{"mykey"}$

字母序号		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
密文编码	C=	16	11	12	18	1	16	24	23	7	1	16	0	24	7	2
密钥编码	k=	12	24	10	4	24	12	24	10	4	24	12	24	10	4	24
加密	C=	4	-13	2	14	-23	4	0	13	3	-23	4	-24	14	3	-22
模运算			13			3					3		2			4
密文解码	C=	e	n	c	o	d	e	a	n	d	d	e	c	o	d	e

Vigenère密码的安全性

- 强度在于：每个明文字母对应着多个密文字母，明、密文字母不是一一对应关系
- 字母的统计规律进一步降低
- **Vigenère**本人建议：密钥与明文一样长
- 特例：
 - 当 $k_1 = k_2 = \dots = k_n = k$ 时，是**Caesar**密码

异或（**Exclusive-or**）加密（**Vernam**）

XOR Operation \oplus :

encryption:

$$C_i = P_i \oplus k_i$$

Decryption:

$$P_i = C_i \oplus k_i$$

Where

P_i = i^{th} binary digit of plaintext

k_i = i^{th} binary digit of key

C_i = i^{th} binary digit of ciphertext

一次一密



- 随机密钥
- 安全强度取决于密钥的随机性
- 理论上不可破
- 实际上不可行
 - 产生大量的随机密钥难
 - 密钥分配与保护更难

置换密码

Transposition Ciphers

栅栏技术

- 思想：以列（行）优先写出明文，以行（列）优先读出各字母作为密文
 - 例1：先行后列
 - 例2：先列后行

例：栅栏密码(Rail Fence cipher)

- 明文：meet me after the toga party
- 写作：

m e m a t r h t g p r y
e t e f e t e o a a t



- 读出密文为：

MEMATRHTGPRYETEFETEOAAT

改进

- 带有密钥
- 再改进：重复加密，多步置换

例：行移位密码 Row Transposition Ciphers

- 更加复杂的移位
- 以指定的行将明文写作多行
- 按照密钥指定的列读出

○ **Key:**

○ **Plaintext:**

○ **Ciphertext:**

**TTNAAPTMTSUOAOD
WCOIXKNLYPETZ**

3	4	1	2	5	6	7
a	t	t	a	c	k	p
o	s	t	p	o	n	e
d	u	n	t	i	l	t
w	o	a	m	x	y	z

转轮密码

- 在现代密码之前，转轮密码是最广泛使用的复杂的密码
- 广泛用在第二次世界大战中
 - **German Enigma, Allied Hagelin, Japanese Purple**
- 实现了复杂多变的多表代替密码，多层加密
- 采用一系列转轮，每一个都是一个代替表，转轮可以依次旋转加密每个字母
 - 用**3**个转轮就有 **$26^3=17576$** 代替表

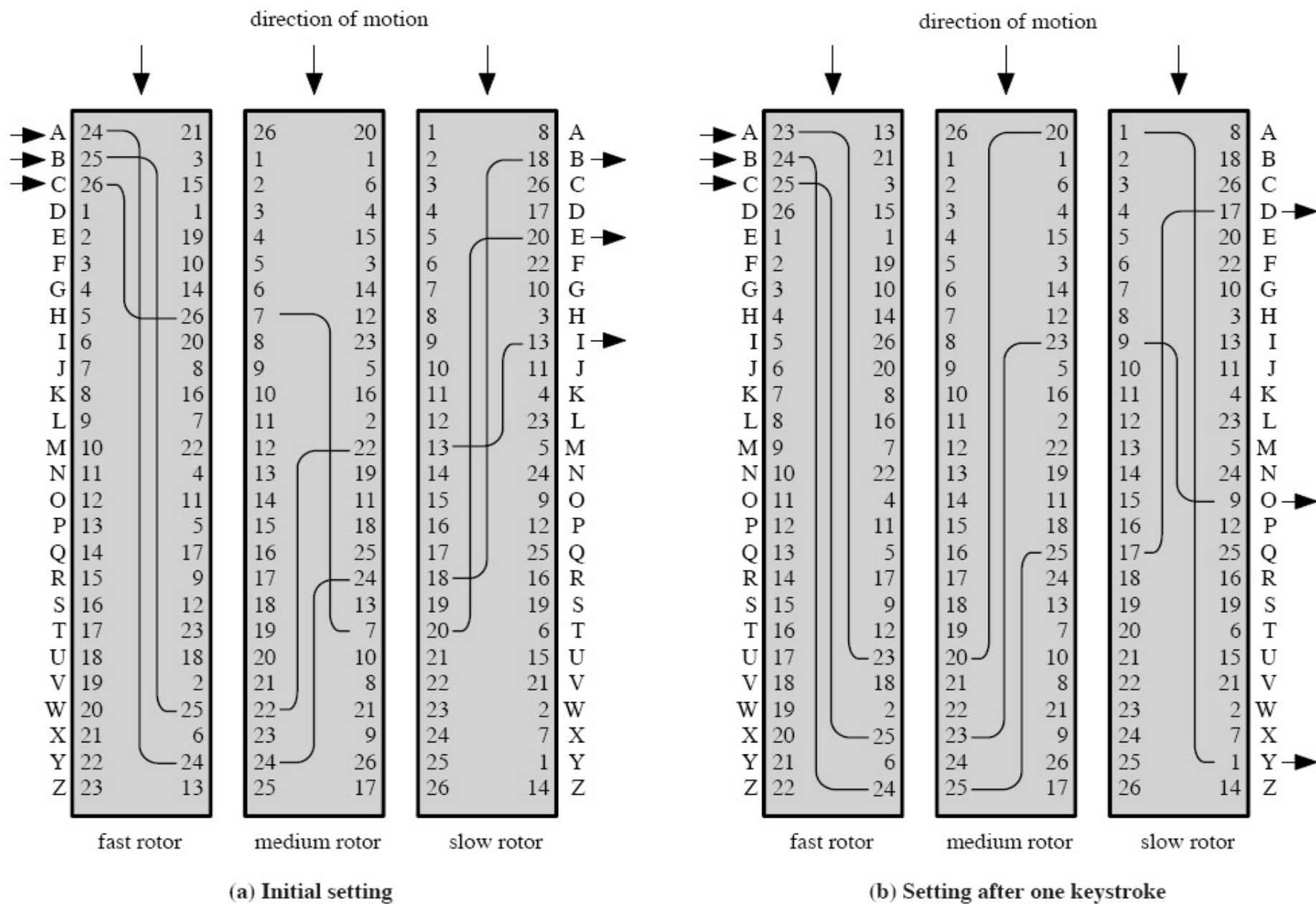
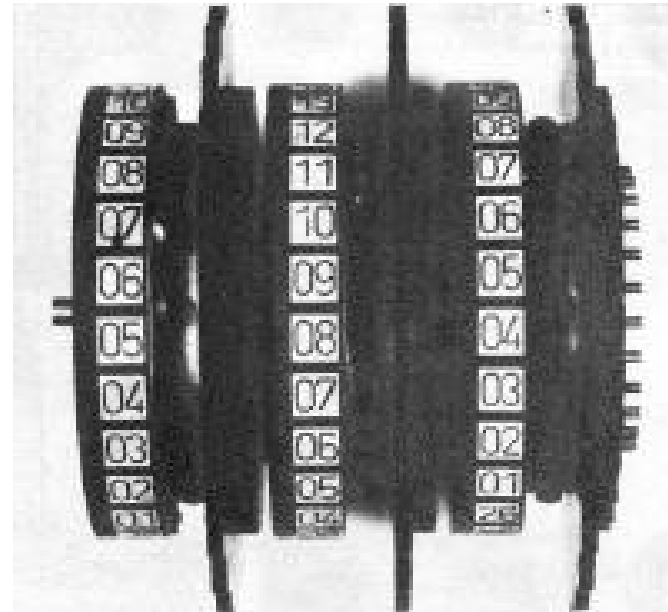
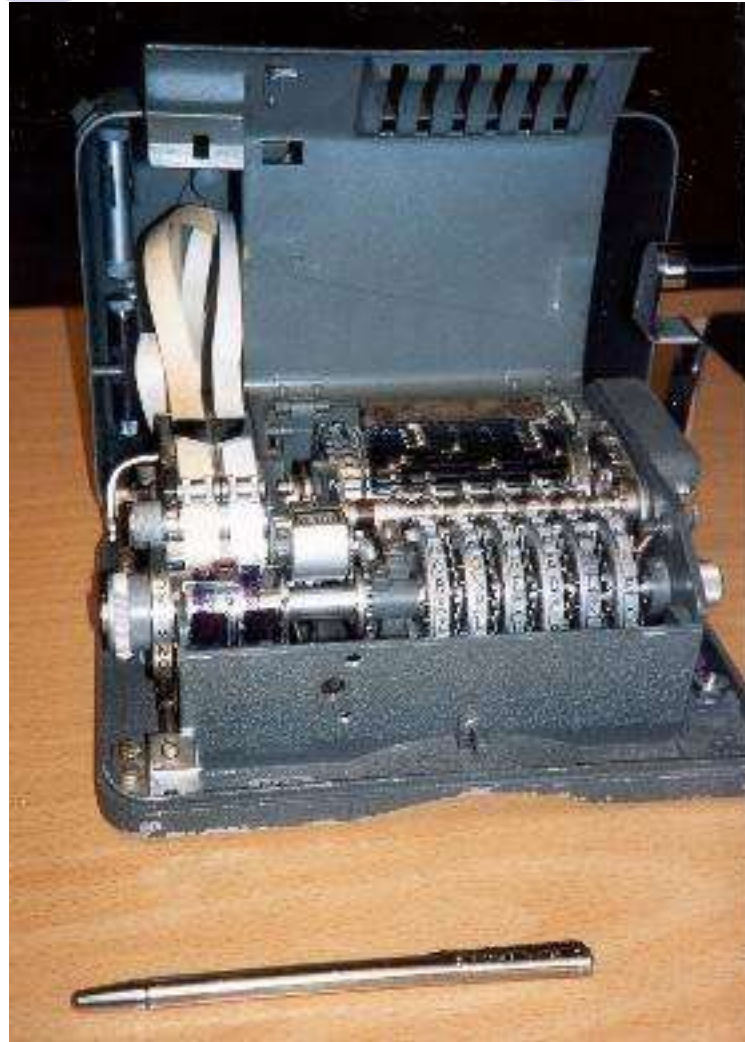


Figure 2.7 Three-Rotor Machine With Wiring Represented by Numbered Contacts

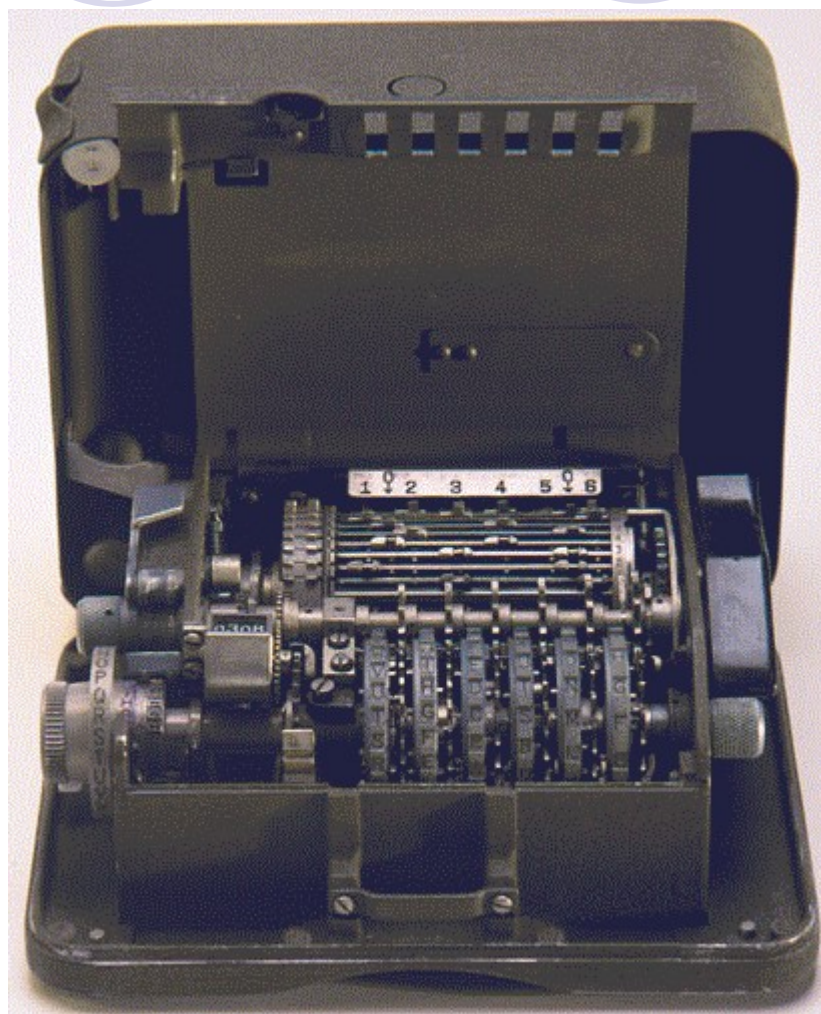
Enigma 密码机(德国)



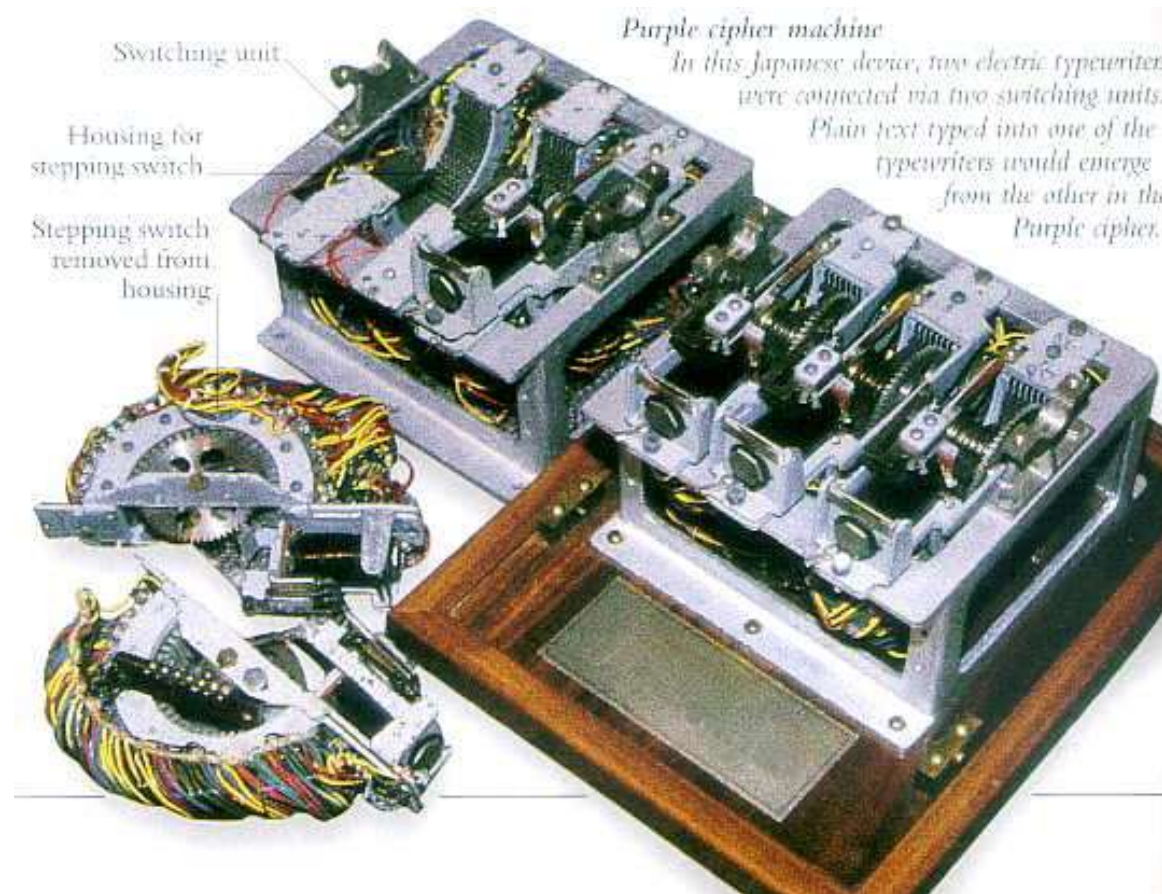
Hagelin 转轮密码机（盟军）



M-209 密码机（美国）



Purple 密码机（日本）



隐写术

Steganography

- 隐藏信息的存在
 - “藏头诗”
 - 字符标记
 - 用不可见的墨水
 - 打字机的色带校正
 - 数字水印
- 缺点
 - 需要额外的付出来隐藏相对较少的信息

隐写术

3rd March

Dear George,

Greetings to all at Oxford. Many thanks for your letter and for the Summer examination package. All Entry Forms and Fees Forms should be ready for final despatch to the Syndicate by Friday 20th or at the very latest, I'm told, by the 21st. Admin has improved here, though there's room for improvement still; just give us all two or three more years and we'll really show you! Please don't let these wretched 16+ proposals destroy your basic O and A pattern. Certainly this sort of change, if implemented immediately, would bring chaos.

Sincerely yours.

A Puzzle for Inspector Morse
(From The Silent World of Nicholas Quinn, by Colin Dexter)