现代密码学理论与实践

第2章 传统加密技术

密码学的演变历史(1)
William Friedman

- 1918, William Friedman's The Index of Coincidence and its Applications in Cryptography
- **William Frederick Friedman** (Sept. 24,1891 – Nov. 12, 1969) 美国陆军密码专家。1930年代，他领导了陆军的一个研究部门Signals Intelligence Service (SIS)，其中一部分服务一直延续到五十年代。三十年代晚期，在他的指导下，Frank Rowlett破解了日本人的PURPLE加密机(紫密)，截获了日本的大量外交和军事的秘密。

密码学的演变历史(2) 香农的贡献

- 1948年, Claude Shannon’s发表“The Communication Theory of Secrecy System”成为现代密码学理论基础。
- 1949年，Shannon在其著名的“信息论” 发表一年之后，又发表了论文“保密系统的通信理论”， 首次将密码学研究置于坚实的数学基础上。
- 该理论的重大贡献在于：
  - 建立了通信保密/密码学严格的理论基础；
  - 证明了一次一密(one-time pad)的密码系统是完善保密的，导致了对流密码的研究和应用；
  - 提出分组密码设计应该遵循的准则，如扩散性和混淆性；
  - 证明了消息冗余使得破译者统计分析成功的理论值(唯一解距离)

密码学的演变历史(2)

- Claude Elwood Shannon (Apr. 30, 1916 – Feb. 24, 2001), 美国电气工程师和数学家，被誉为信息论之父 "the father of information theory".
- 香农之有名在于他以1948年发表的那篇旷世论文而奠定了现代信息论基础。其实早在1937年，当21岁的香农还是MIT的硕士研究生时，他便在他的硕士论文中论述了布尔代数的电子实现和应用，可以构建和解决任何逻辑的和数字的关系，因此奠定了数字计算机和数字电路设计理论的基础。他的硕士论文一直被认为是迄今最重要的硕士论文。
- 1949-1967，密码学研究处于沉寂时期

密码学的演变历史(3)

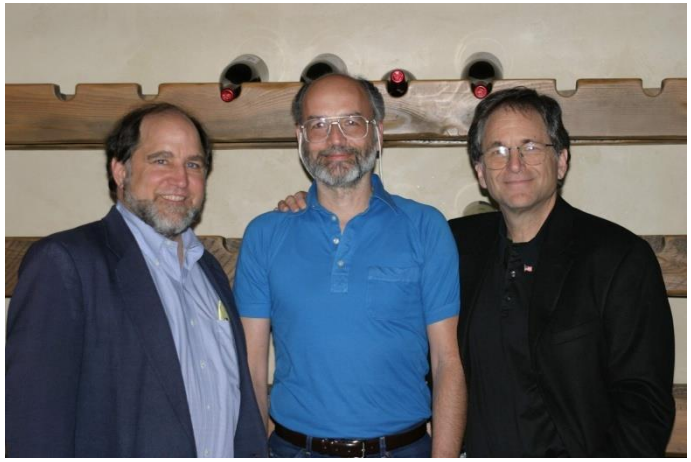
Feistel, Whitfield Diffie, Matin Hellman

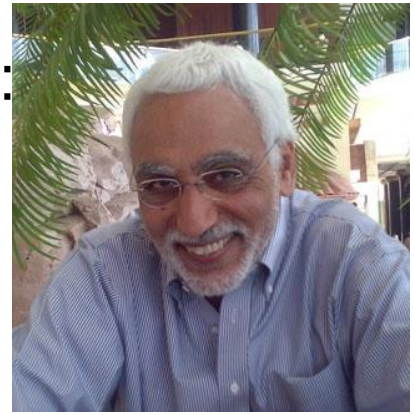
- 1971, IBM发明Luciffer Cipher, 128位密钥作分组加密。这项发明是由Horst Feistel(Jan.30, 1915–Nov.14,1990)领导的，他是密码学家，当时在IBM负责设计加密器，他的工作最终激发了70年代Data Encryption Standard (DES)的研发高潮
- 1976-1977，美国国家标准局正式公布实施DES
- 1975, Whitfield Diffie 和 Matin Hellman, 发表A New Direction in Cryptography, 首次提出适应网络保密通信的公开密钥思想，揭开现代密码学研究的序幕，具有划时代的意义

密码学的演变历史(4)

R.S.A., Abbas El Gamal, Lai Xuejia

- 1977-1978，Ronald Rivest, Adi Shamir, Len Adleman第一次提出公开密钥密码系统的实现方法RSA
- 1981，成立International Association for Cryptology Research
- 1985，Abbas El Gamal提出概率密码系统ElGamal方法
- 1990-1992，Lai Xuejia and James: IDEA, The International Data Encryption Algorithm
- 2000, AES, Advanced Encryption Standard

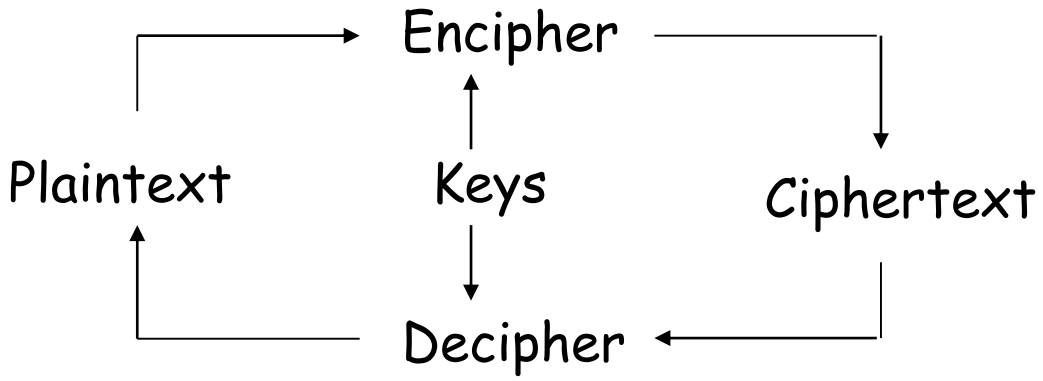




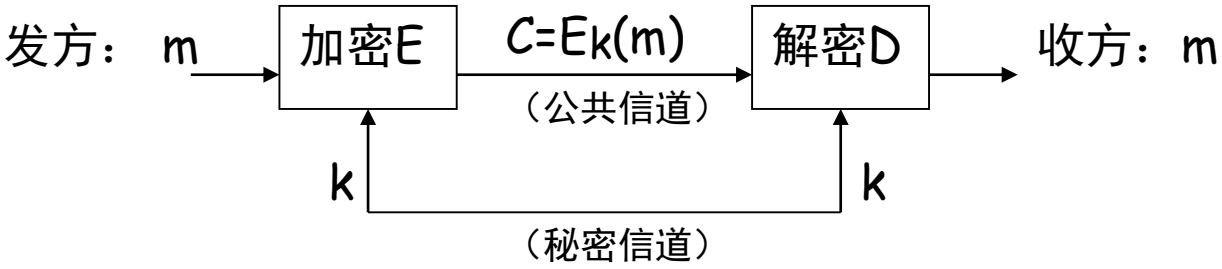
密码学基本术语 Terminologies

- Cryptology(保密学)，源自希腊语(Greek)
  Kryptós: hidden; logos: word, 是密码学和密码处理过程的研究
- Cryptography: The Science and Study of Secret Writing，密码编码学
- Cryptanalysis: The Science and Study of Secret Breaking，密码破译学
- Cipher: A secret method of writing 加密方法
- Encipher (encipherment), encryption: 将明文转换成密文的过程
- Decipher (decipherment), decryption: 将密文还原成明文的过程
- Plaintext (cleartext): 原始的可读数据，明文
- Ciphertext (Cryptogram): 加密后的不可解读之文件，密文
- Key: 密钥，对加密与解密过程进行控制的参数
- E(m): Encryption Transformation 加密变换
- D(c): Decryption Transformation 解密变换

简单加密系统模型



- 什么是密码？简单地说它就是一组含有参数K的变换E。设已知消息m，通过变换E_k得密文C，这个过程称为加密，E为加密算法，k不同，密文C亦不同。传统的保密通信机制：



理论安全和实际安全

- 理论安全，或无条件安全Theoretical Secure (or Perfect Secure)

  攻击者无论截获多少密文，都无法得到足够的信息来唯一地决定明文。Shannon用理论证明：欲达理论安全，加密密钥长度必须大于等于明文长度，密钥只用一次，用完即丢，即一次一密，One-time Pad，不实用。
- 实际安全，或计算上安全Practical Secure (or Computationally Secure)

  如果攻击者拥有无限资源，任何密码系统都是可以被破译的；但是在有限的资源范围内，攻击者都不能通过系统的分析方法来破解系统，则称这个系统是计算上安全的或破译这个系统是计算上不可行(Computationally Infeasible)。

加密的基本概念

- 密码体制
  - 加密系统采用的基本工作方式称为密码体制，密码体制的基本要素是密码算法和密钥。密码算法是一些公式、法则或程序；密钥是密码算法中的控制参数。
  - 加密系统可以用数学符号来描述：

    $S=\{P, C, K, E, D\}$

    P：明文空间　　C：密文空间　K：密钥空间

    E：加密变换　　D：解密变换　$k \in K$，

    则有$C=E_k(P)$，$P=D_k(C)=D_k(E_k(P))$，

    或者$D_k=E_k^{-1}$，且$E_k=D_k^{-1}$。

对称密码体制和非对称密码体制

- 对称密码体制(Symmetric System, One-key System, Secret-key System)

  加密密钥和解密密钥相同，或者一个密钥可以从另一个导出，能加密就能解密，加密能力和解密能力是结合在一起的，开放性差。

- 非对称密码体制(Asymmetric System, Two-key System, Public-key System)

  加密密钥和解密密钥不相同，从一个密钥导出另一个密钥是计算上不可行的，加密能力和解密能力是分开的，开放性好。

序列密码体制和分组密码体制

- 序列密码
  - 如果密文不仅与最初给定的算法和密钥有关，同时也与明文位置有关(是所处位置的函数)，则称为序列密码体制。加密以明文比特为单位，以伪随机序列与明文序列模2加后，作为密文序列。
- 分组密码
  - 如果经过加密所得到的密文仅与给定的密码算法和密钥有关，与被处理的明文数据在整个明文中的位置无关，则称为分组密码体制。通常以大于等于64位的数据块为单位，加密得相同长度的密文。

其他加密体制

- 确定型密码体制和概率密码体制
  - 确定型：当明文和密钥确定后，密文也就唯一地确定了；
  - 概率型：当明文和密钥确定后，密文通过客观随机因素从一个密文集合中产生，密文形式不确定，称为概率型密码体制。
- 单向函数型密码体制和双向变换型密码体制
  - 单向函数型密码体制适用于不需要解密的场合，容易将明文加密成密文，如哈希函数；
  - 双向变换型密码体制可以进行可逆的加密、解密变换。

现代密码学基本原则及加密系统要求

- 现代密码学的基本原则
  - 设计加密系统时，总是假定密码算法是可以公开的，需要保密的是密钥。一个密码系统的安全性不在算法的保密，而在于密钥，即Kerckhoff原则。
- 对加密系统的要求
  - 系统应该是实际上安全的(practical secure)，截获密文或已知明文－密文对时，要决定密钥或任意明文在计算上是不可行的。
  - 加密解密算法适用于密钥空间中的所有元素。
  - 系统易于实现，使用方便。
  - 系统的安全性不依赖于对加密体制或加密算法的保密，而依赖于密钥。
  - 系统的应用不应使通信网络的效率过分降低。

2.1 对称密码系统的模型

- 对称加密系统由以下五部分组成
  - Plaintext： 明文
  - Encryption algorithm：加密算法
  - Key： 密钥
  - Ciphertext：密文
  - Decryption algorithm：解密算法
- 加密算法必须足够强大，使破译者不能仅根据密文破译消息
- 收发双方必须在某种安全的形式下获得密钥并必须保证密钥的安全

传统密码的简化模型

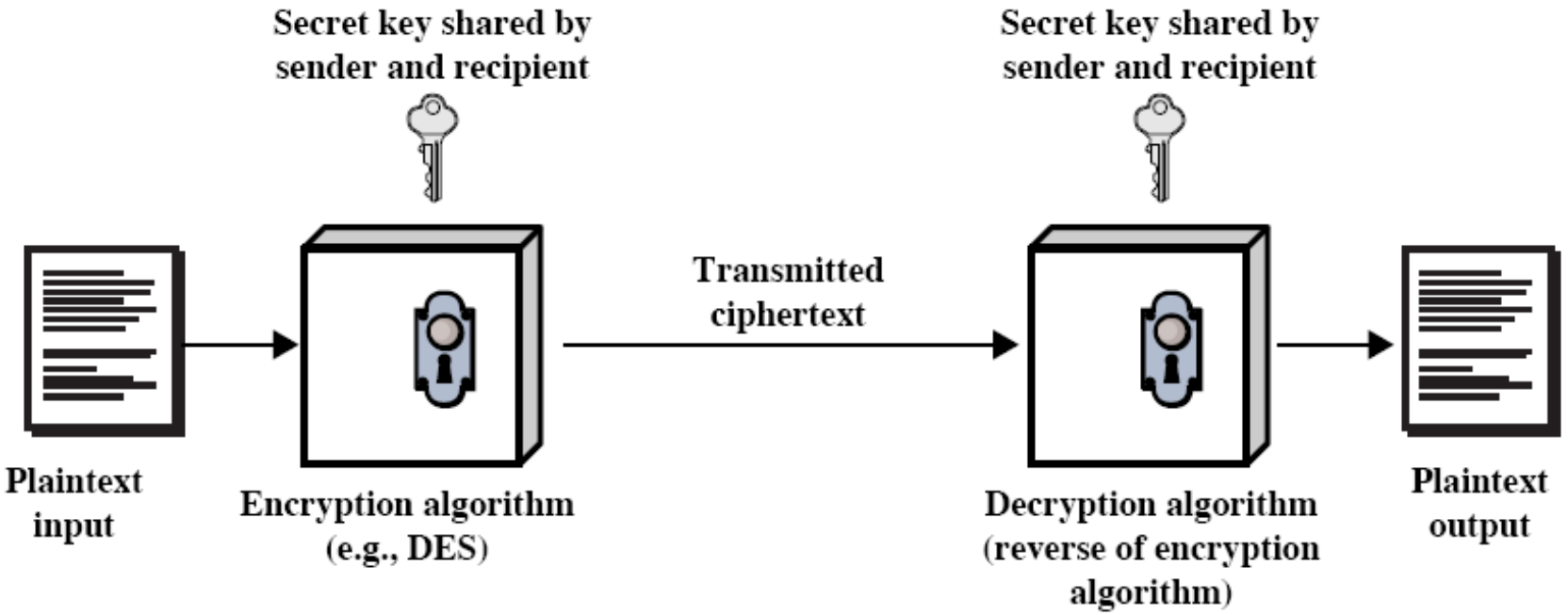


Figure 2.1 Simplified Model of Symmetric Encryption

对称密码系统的要求

- 使用对称密码系统有两个基本要求
  - 一个强加密算法
  - 一个只有发送方和接收方知道的秘密密钥

  $Y = E_K(X)$

  $X = D_K(Y)$
- 必须假定加密算法是公开的
- 因此必须有安全的途径或信道分发密钥

传统密码体制的模型

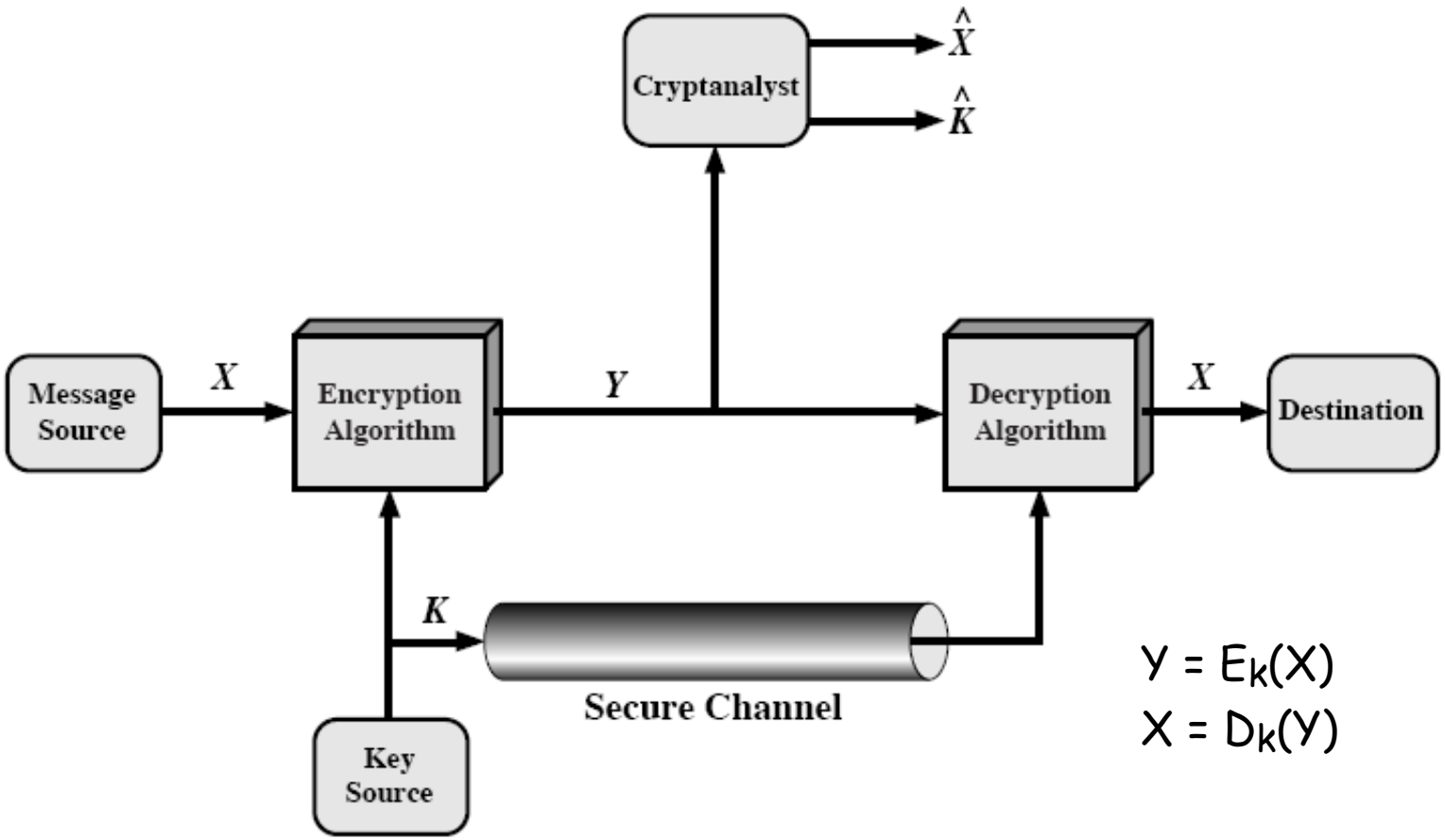


Figure 2.2 Model of Symmetric Cryptosystem

Cryptology 密码学

- 密码编码学(Cryptography)

  密码编码系统根据以下三个独立方面进行分类
  - 用于将明文转换为密文的操作类型：代换和置换
  - 所使用的密钥的数量和方式：
    - 对称密码体制(单钥系统、秘密密钥系统)
    - 非对称密码体制(双钥系统、公开密钥系统)
  - 明文的处理方式：分组加密和流加密
- 密码分析学(Cryptanalysis)
  - 密码分析：试图破译密文得到明文或试图获得密钥的过程为密码分析，密码破译的策略取决于加密方法及可供破译者使用的信息。
  - 穷举攻击：对密文尝试所有可能的密钥，直到把它转化为可读的有意义的明文，至少要尝试1/2种所有可能的密钥。

对加密信息的攻击类型

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

Table 2.1 Types of Attacks on Encrypted Messages

Type of Attack	Known to Cryptanalyst
Ciphertext only	•Encryption algorithm •Ciphertext
Known plaintext	•Encryption algorithm •Ciphertext •One or more plaintext-ciphertext pairs formed with the secret key
Chosen plaintext	•Encryption algorithm •Ciphertext •Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key
Chosen ciphertext	•Encryption algorithm •Ciphertext •Purported ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key
Chosen text	•Encryption algorithm •Ciphertext •Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key •Purported ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key

穷举攻击

- 总是可以简单地尝试每一个可能的密钥
- 穷举攻击是最基本的攻击，难度与密钥长度成正比
- 平均来说要获得成功必须尝试所有可能密钥的一半

Table 2.2 Average Time Required for Exhaustive Key Search

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

2.2 代换密码(Substitution)

- 代换法是将明文字母替换成其他字母、数字或符号的加密方法
- 如果把明文看成是二进制序列的话，代换就是用密文位串来代换明文位串
- 代换法改变明文内容的表示形式，保持内容元素之间相对位置不变
- 已知最早的代换密码是由Julius Caesar发明的恺撒密码Caesar Cipher，对字母表中的每个字母用它之后的第3个字母来代换。例如：

meet me after the toga party

PHHW PH DIWHU WKH WRJD SDUWB

2.2.1 Caesar Cipher

- Caesar实际上是一种单表代换密码

  明文字母用密文字母表中对应字母代替，例：

  明文字母表 $P=\{p_0, p_1, \ldots, p_{n-1}\}$

  密文字母表 $C=\{c_0, c_1, \ldots, c_{n-1}\}$

  密钥为正整数k，加密：$i+k \equiv j \pmod n$

  解密：$j-k \equiv i \pmod n$

  Caesar Cipher，加密：$C = E(p)=(p+k) \bmod 26$

  解密：$p = D(C)=(C-k) \bmod 26$,

  0—A；1—B；…；25—Z

Caesar Cipher

- 定义如下变换

```
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
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
```

- 让每个字母等价于一个数值

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

- Caesar密码可以表示如下

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

  $p = D(C) = (C - k) \bmod (26)$，这里$k = 3$

对Caesar密码的攻击

- 如果已知某给定密文是Caesar密码，穷举攻击是很容易实现的，因为只要简单地测试所有25种可能的密钥
- Caesar密码的三个重要特征使我们可以采用穷举攻击分析方法
  - 已知加密和解密算法
  - 所需测试的密钥只有25个
  - 明文所用的语言是已知的，且其意义易于识别
- 比如，破解密文**PHHW PH DIWHU WKH WRJD SDUWB**，或者，**GCUA VQ DTGCM**

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 toga party
4	ldds ld zesdq sgd snfz ozqsx
5	kccr kc ydrcp rfc rmey nyprw
6	jbbq jb xcqbo qeb qldx mxoqv
7	iaap ia wbpan pda pkcw lwnpu
8	hzzo hz vaozm ocz ojbv kvmot
9	gyyn gy uznyl nby niau julns
10	fxxm fx tymxk max mhzt itkmr
11	ewwl ew sxlwj lzw lgys hsjlq
12	dvvk dv rwkvi kyv kfxr grikp
13	cuuj cu qvjuh jxu jewq fqhjo
14	btti bt puitg iwt idvp epgin
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 glzkx znk zumg vgxze
24	rjjy rj fkyjw ymj ytlf ufwyd
25	qiix qi ejxiv xli xske tevxc

Figure 2.3 Brute-Force Cryptanalysis of Caesar Cipher

对Caesar密码的攻击

- 如果明文所用语言不为我们所知，则明文输出不可识别，而且输入可能按某种方式经过缩写或压缩，则识别就更加困难
- 例如

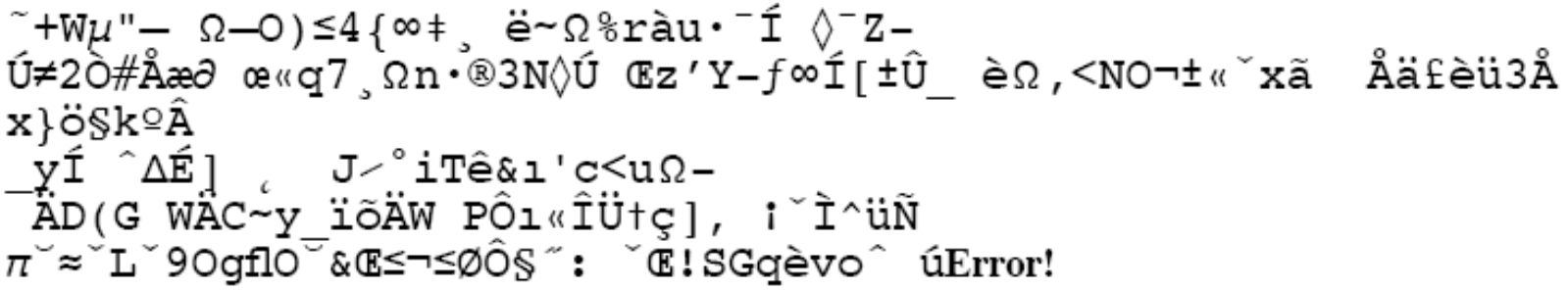


Figure 2.4 Sample of Compressed Text

2.2.2 Monoalphabetic Cipher
单表代换密码

- 单表代换密码不只是25种可能的密钥，而是允许任意代换，增加密钥空间
- 每个明文字母可以随机映射到任意一个密文字母，密文行是26个字母的任意置换，那么有26!或大于$4x10^{26}$种可能的密钥，每条消息用一个字母表加密
- 这样密钥有26个字母长

```
Plain:  abcdefghijklmnopqrstuvwxyz
Cipher: DKVQFIBJWPESCXHTMYAUOLRGZN
Plaintext:  ifwewishtoreplaceletters
Ciphertext: WIRFRWAJUHYFTSDVFSFUUFYA
```

单表代换密码的安全性分析

- 只要密文字符是26个字母的一个排列即可。
- 单表代换密码中每条消息用一个字母表加密
- 这样有26! = $4x10^{26}$种可能的密钥，超过400,000,000,000,000,000,000,000,000

  $4x10^{26}$ = 400万亿亿
- 这比DES的密钥空间大10个数量级，看起来是安全的，应该可以抵御穷举攻击，其实不然
- 这是因为语言的一些规律和特性

语言的冗余性和密码攻击

- 人类的语言是有冗余性的
  - 比如从“th lrd s m shphrd shll nt wnt”中我们可以大概猜出些什么
- 字母使用的频率是不一样的
  - 英文字母E是使用最频繁的，然后是T, R, N, I, O, A, S等
- 有些字母使用得很少，如Z, J, K, Q, X
  - 这样可以得到英文字母使用频率分布表
- 同时，统计双字母组合和三字母组合的使用频率也是非常有用的

英文字母的相对使用频率

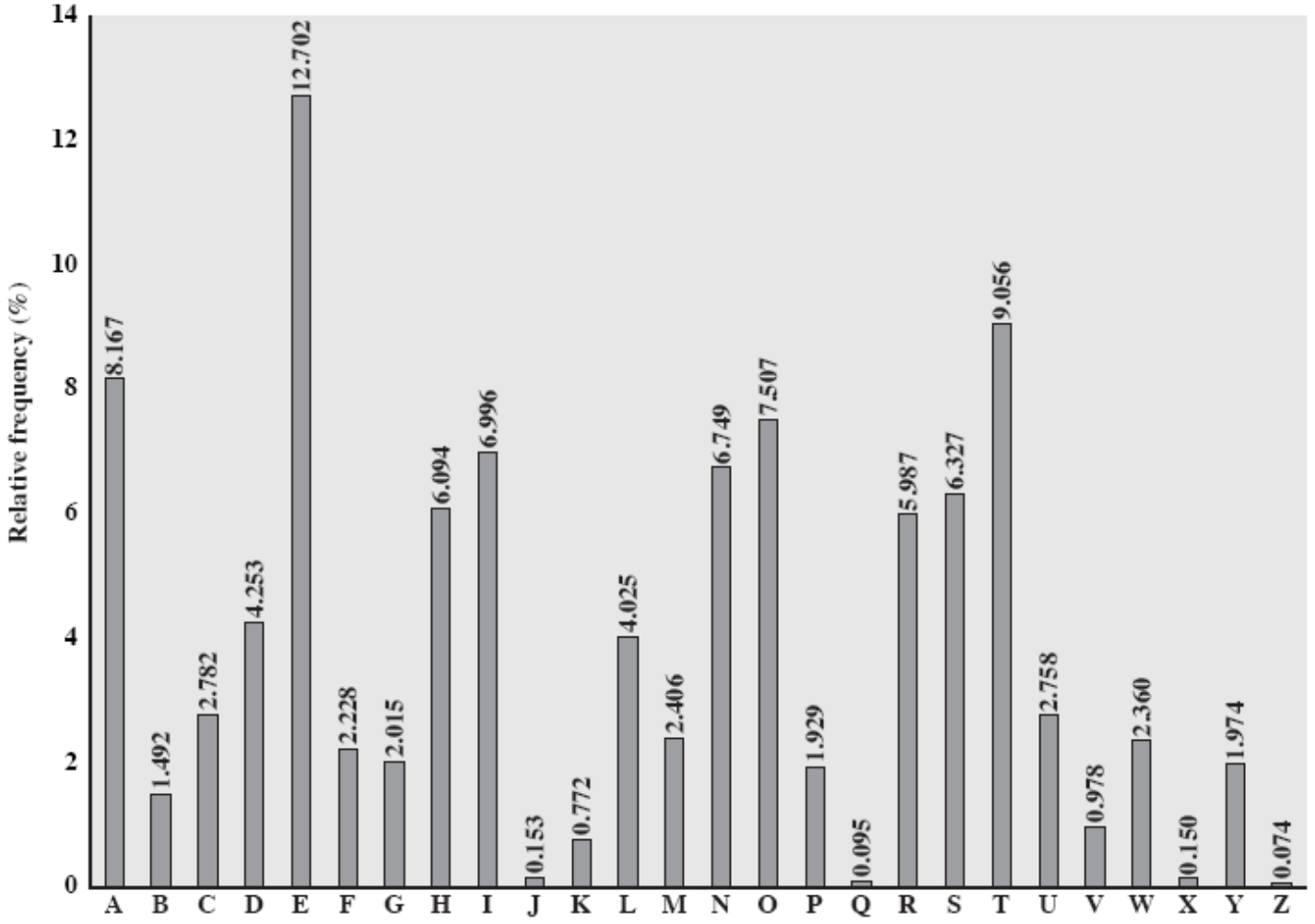


Figure 2.5 Relative Frequency of Letters in English Text

英文字母使用频率用于密码分析

- 关键的一点，单表代换不能改变相关字母出现的频率
- 这是由阿拉伯科学家在公元九世纪就分析发现了
- 所以，只要统计密文中字母出现的频率，与已知的统计值做比较就可以分析出相应明文字母了
- 如果Caesar密码中字母呈现出通常的峰值和低谷，那么单表代换也会呈现相同的特性，比如：
  - 峰值在：A-E-H-I, N-O, R-S-T
  - 低谷在：J-K, Q, X-Z
- 双字母、三字母出现特性表也会有助于破译密文

单表代换密码攻击举例

- 给定密文:

  UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ

  VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX

  EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ

- 统计相关字母出现的次数 (see textbook)
- 可以猜测P和Z是e和t，ZW是th，这样ZWP就是the
- 这样反复试验并不断修正错误，最后可得:

  it was disclosed yesterday that several informal but direct contacts have been made with political representatives of the viet cong in moscow

2.2.3 Playfair密码

- 单表代换尽管有大量的密钥，也不能提供足够的安全性，因为密文中残留了大量的明文结构，一种解决办法是引进多表代换密码。
- Playfair密码是最著名的多表代换密码，它把明文中的双字母音节作为一个单元转换成密文的双字母音节。
- Playfair密码是由英国科学家Charles Wheatstone在1854年发明的，用了他的朋友Baron Playfair的名字命名。
- Playfair算法基于一个由密钥词构成的5x5字母矩阵

PLAYFAIR密码的密钥矩阵

- 假定使用的密钥词是MONARCHY
- 先在5x5矩阵中填上密钥词，去掉重复字母
- 再将剩余的字母按字母表的顺序从左至右、从上至下填在矩阵剩下的格子中，I和J当作一个字母

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密码的加密

- 对明文按如下规则一次加密两个字母
  1. 如果该字母对的两个字母是相同的，则在其中插入一个填充字母，如 ‘x’, “balloon”加密成“ba lx lo on”
  2. 落在同一行的明文字母对中的字母由其右边的字母来代换，每行中最右的字母用该行最左边的第一个字母来代换, 如 “ar”加密成“RM”
  3. 落在同一列的明文字母对中的字母由其下面的字母来代换，每列中最下面的一个字母用该列最上面的第一个字母来代换, 如 “mu”加密成“CM”
  4. 其他的每组明文字母对中的字母按如下方式代换：该字母所在行为密文所在行，另一字母所在列为密文所在列，如 “hs”变换成“BP”， “ea”代换为“IM”或“JM” (as desired)

Playfair密码的安全性

- Playfair密码安全性比单表代换大为提高
- 因为有26个字母，因此有26 x 26 = 676字母对，对单个字母对进行判断要困难得多。
- 单个字母的相对频率比字母对的相对频率在统计规律上要好，利用频率分析字母对就更困难些，需要676输入的频率表来进行分析。
- 被广泛地使用了许多年，包括在一战和二战时期。英国军队使用了一个世纪，曾保证是安全的，但1915年被德军破译。1941年起，德军和盖世太保使用双表playfair，1944年秋季被英国的Bletchey Park破译。
- 因为它的密文仍然完好地保留了明文语言的大部分结构特征，它仍然是相对容易攻破的，几百个字母的密文就足够分析出规律了。

字母出现的相对频率

- “明文”曲线画出7万个字母的频率分布，对文中出现的每个字母计数，结果除以字母e的出现次数。
- 加密后的曲线体现了加密后字母频率分布被掩盖的程度，如果完全被掩盖，则应该是一条水平线。

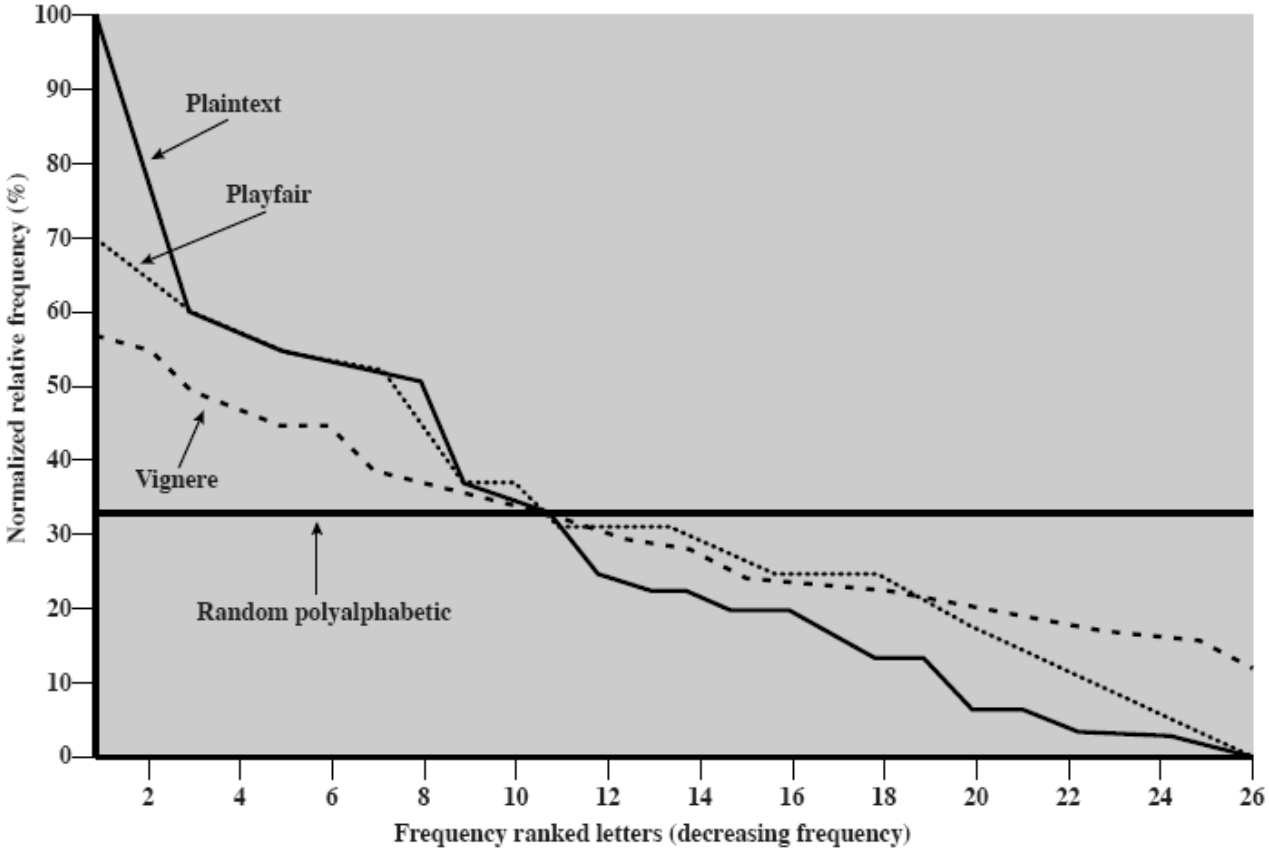


Figure 2.6 Relative Frequency of Occurrence of Letters

2.2.4 Hill密码

- 1929年数学家Lester Hill发明Hill密码
- 将m个连续的明文字母替换成m个密文字母，这由m个线性方程决定，每个字母指定一个数值(a=0, b=1，…, z=25)，假如m为3：
  - $c_1=(k_{11}p_1+k_{12}p_2+k_{13}p_3) \bmod 26$
  - $c_2=(k_{21}p_1+k_{22}p_2+k_{23}p_3) \bmod 26$
  - $c_3=(k_{31}p_1+k_{32}p_2+k_{33}p_3) \bmod 26$
- 用列向量和矩阵表示为

$$\begin{pmatrix} c_1 \\ c_2 \\ c_3 \end{pmatrix} = \begin{pmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{pmatrix} \begin{pmatrix} p_1 \\ p_2 \\ p_3 \end{pmatrix} \bmod 26$$

或 $C=KP \bmod 26$

*C*和*P*是长度为3的列向量，分别代表密文和明文

*K*是一个3x3矩阵，代表加密密钥，运算按模26执行

HILL密码

- 明文paymoremoney，加密密钥为

$$\mathbf{K} = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$$

  - 明文前三个字母用向量[15 0 24]表示，则

$$\begin{pmatrix} 15 \\ 0 \\ 24 \end{pmatrix}. \text{Then } \mathbf{K}\begin{pmatrix} 15 \\ 0 \\ 24 \end{pmatrix} = \begin{pmatrix} 375 \\ 819 \\ 486 \end{pmatrix} \bmod 26 = \begin{pmatrix} 11 \\ 13 \\ 18 \end{pmatrix} = \text{LNS}$$

  - 照此转换剩下字母，可得密文LNSHDLEWMTRW

- 解密需要用到矩阵K的逆K^{-1}，由$KK^{-1}=I$ 定义，I是单位矩阵

HILL密码

$$\mathbf{K} = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \qquad \mathbf{K}^{-1} = \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix}$$

- $KK^{-1} = I$ 可以验证如下

$$\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} = \begin{pmatrix} 443 & 442 & 442 \\ 858 & 495 & 780 \\ 494 & 52 & 365 \end{pmatrix} \bmod 26 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

- Hill密码系统可以表示如下
  - $\boldsymbol{C}=\mathrm{E}(\boldsymbol{K}, \boldsymbol{P})=\boldsymbol{KP} \bmod 26$
  - $\boldsymbol{P}=\mathrm{D}(\boldsymbol{K}, \boldsymbol{C})=\boldsymbol{K}^{-1}\boldsymbol{C} \bmod 26=\boldsymbol{K}^{-1}\boldsymbol{KP}=\boldsymbol{P}$

2.2.5 Polyalphabetic Ciphers
多表代换密码

- 改进简单的单表代换的方法是在明文消息中采用不同的单表代换，这就是多表代换密码poly-alphabetic substitution ciphers
- 因为需要猜测更多的字母表，并且频率分布特性也变得平坦了，所以使得密码破译更加困难
- 使用一密钥词对每个明文字母选择一个字母表来加密
- 依次使用每个字母表
- 如果到了密钥词最后一个字母，则从头开始继续

Vigenère密码

- 最简单的多表代换密码是Vigenère密码，它其实是多重Caesar密码
- 26个密码水平放置，最左边是密钥字母，顶部排列的是明文的标准字母表
- 加密一条消息需要与消息一样长的密钥，密钥是密钥词的重复，比如，密钥词为$K = k_1\ k_2\ \ldots\ k_d$
- 加密：给定密钥字母x和明文字母y，密文字母是位于x行和y列的那个字母
- 密钥词的第*i* 字母，表明使用第*i*个字母表，轮流使用字母表，如果到了消息的第*d*个字母时则从头再做
- 解密：密钥字母决定行，行里密文字母所在列的顶部字母就是明文字母

Table 2.3 The Modern Vigenère Tableau

Key \ 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

Example

- 写下明文
- 在明文之上重复写下密钥
- 像使用Caesar cipher密钥那样使用每一个密钥字母，加密每一个明文字母
- 比如，使用密钥*deceptive*

```
key:        deceptivedeceptivedeceptive
plaintext:  wearediscoveredsaveyourself
ciphertext:ZICVTWQNGRZGVTWAVZHCQYGLMGJ
```

Vigenère密码的安全性

- 每一个明文字母可以有多个密文字母对应，这样字母使用的频率特性减弱了，但是没有完全消失
- 攻击者首先要分析密文是否是用单表代换加密的，即通过简单的测试密文的统计特性
- 如果认为是用Vigenère密码加密的，破译能否取得进展将取决于能否判定密钥词的长度，要通过发现重复序列来判断
- 如果密钥词长度是N，那么密码实际上包含了N个单表代换
- 密钥词的周期性可以用与明文信息一样长的不重复密钥词来消除，如“密钥自动生成系统”，但是密文和明文具有相同频率分布特性，仍然是易受攻击的
- 最终措施是选择与明文毫无统计关系且和它一样长的密钥

Kasiski Method to break Vigenère
卡西斯基方法破解Vigenère

- 破解Vigenère的方法是由Charles Babbage(巴贝奇)和Friedrich Kasiski(卡西斯基)分别发现的
- 密文中的重复性可以暗示出密钥词长度
- 如果两个相同明文序列之间的距离是密钥词长度的整数倍，那么产生的密文序列也是相同的
- 前例中“red”的两次出现相隔9个字母，因此得到了两个相同密文序列VTW
- 这时攻击者就可以猜测密钥词的长度是3或者9
- 这样攻击者可以像先前攻击单表密码那样分别进行攻击
- 密钥词的周期性可以用与明文信息一样长的不重复密钥词来消除，Autokey Cipher

Autokey Cipher

- 最理想的是让密钥和要加密的消息一样长
- Vigenère提出了**autokey cipher**，密钥词keyword放在消息前面作为密钥key前缀
- 知道了密钥词能够破译密文的前面一些字母，据此可以解密密文消息的其余部分
- 但是这种方法仍然具有字母使用的频率特性可供分析
- 例如，给定密钥词：*deceptive*

```
key:        deceptivewearediscoveredsav
plaintext:  wearediscoveredsaveyourself
ciphertext:ZICVTWQNGKZEIIGASXSTSLVVWLA
```

2.2.6 One-Time Pad一次一密

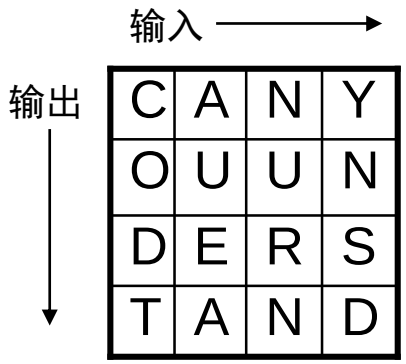
- Joseph Mauborgne提出使用与消息一样长且无重复的随机密钥来加密消息，密钥只对一个消息加解密，之后弃之不用；每条新消息都需要与其等长的新密钥，这就是一次一密，它是不可攻破的。
- 一次一密运算基于二进制数据而非字母
  - 加密：$c_i = p_i \oplus k_i$, p_i是明文第i个二进制位，k_i是密钥第i个二进制位，c_i是密文第i个二进制位，$\oplus$是异或运算
  - 密文是通过对明文和密钥的逐位异或而成的，根据异或运算的性质，解密过程为$p_i = c_i \oplus k_i$,
- 给出任何长度与密文一样的明文，都存在着一个密钥产生这个明文。如果用穷举法搜索所有可能的密钥，会得到大量可读、清楚的明文，但是无法确定哪个才是真正所需的，因而这种密码不可破。
- 一次一密的两个限制
  - 产生大规模随机密钥有实际困难
  - 密钥的分配和保护无法保证

2.3 Transposition Ciphers
置换密码

- 置换密码改变明文内容元素的相对位置，保持内容的表现形式不变
- 通常称为**transposition**或者**permutation**密码
- 通过重新安排消息字母的位置来隐藏明文信息，而不是用其他字母来代换明文字母
- 这种方法是很容易破译的，因为密文拥有与明文一样的字母频率统计特性

Transposition or permutation
置换密码

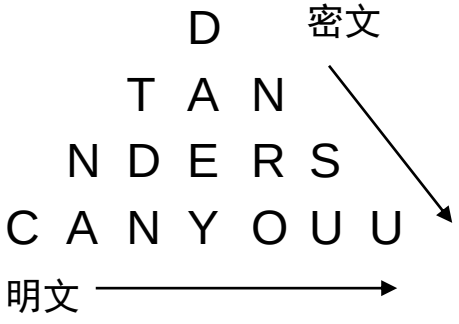
- 一维变换—矩阵转置



明文：can you understand

密文：codtaueanurnynsd

- 二维变换—图形转置



密文：dnsuaruteodynnac

明文：can you understand

栅栏技术 Rail Fence cipher

- 按照对角线的顺序写出明文，按行的顺序读出作为密文
- 如加密 **meet me after the toga party:**

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

  e t e f e t e o a a t
- 可以得到密文

  MEMATRHTGPRYETEFETEOAAT

Row Transposition Ciphers
行置换密码

- 一个更复杂的方案是把消息一行一行地写成矩形块，然后按列读出，但是把列的次序打乱，列的次序就是算法的密钥，例如：
- **Key:** **4 3 1 2 5 6 7**

  Plaintext: **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

  Ciphertext: TTNAAPTMTSUOAODWCOIXKNLYPETZ
- 可以采用多步置换来得到相对较高的安全性

乘积密码Product Ciphers

- 单纯的代换或者置换密码是不安全的，因为语言的特性
- 因此可以考虑连续使用若干这样的密码使其难以破解，但是：
  - 两次代换只生成更复杂的代换
  - 两次置换只生成更复杂的置换
- 如果在一次代换之后跟一次置换，可以生成一种新的更难破解的密码，这就是乘积密码
- 乘积密码是从古典密码通往现代密码的桥梁

2.4 Rotor Machines转轮密码机

- 在现代密码系统出现之前，转轮密码机是最为广泛使用的多重加密器，尤其是在第二次世界大战中。
  - German Enigma, Japanese Purple, Allied Hagelin
- 转轮密码机实现了一个非常复杂、变化多端的代换密码。
- 转轮机使用一组相互独立的旋转圆筒，可以通过电脉冲，每个圆筒有26个输入和26个输出，每个输入仅与一个输出相连，一个圆筒就定义了一个单表代换。
- 每按下一个键，圆筒旋转一个位置，内部连线相应改变，就定义了不同的单表代换密码，经过26个明文字母，圆筒回到初始状态，就得到一个周期为26的多表代换密码。
- 3个圆筒的转轮机就有26^3=17576个不同的代换字母表

Enigma：密码学界划时代的丰碑

- http://www.techcn.com.cn/index.php?doc-view-131925 (科技中国介绍德国发明家亚瑟·谢尔比乌斯)
- Enigma(转轮密码机)在密码学界里，绝对是划时代的丰碑。它所凝聚成的不是一座丰碑，而是两座：研究并制造出Enigma是一座，研究并破解Enigma是另一座。只要稍微了解一下Enigma的历史，我们就会被其中闪耀的人类智慧之美所折服；而如果要向这样辉煌的智慧敬献花环的话，主要应该献给三个人：首先是德国人亚瑟·谢尔比乌斯(Arthur Scherbius)；其次是波兰人马里安·雷耶夫斯基(Marian Rejewski)；然后是英国人阿兰·图灵(Alan Turing)。
- 德国人发明了Enigma；波兰人初步破解了简单的Enigma；而英国人彻底终结了最高难度的Enigma。

亚瑟·谢尔比乌斯和ENIGMA

- 1918年，德国发明家亚瑟·谢尔比乌斯(Arthur Scherbius)和理查德·里特Ritter创办了一家新技术应用公司，利用现代化的电气技术，来取代手工编码加密方法，发明了一种能够自动编码的机器。谢尔比乌斯给自己所发明的电气编码机械取名“恩尼格玛”(Enigma，意为哑谜)。
- 恩尼格玛密码机是一种用于加密与解密文件的密码机。确切地说，恩尼格玛是一系列相似的转子机械的统称，包括了一系列不同的型号。恩尼格玛密码机可以简单分为三个部分：键盘、转子和显示器。

普通的“恩格码”密码机一般只有二至三个转子，而这部德国海军专用的密码机却安装了四个转子，大大增加了保密度和对方破绎的难度。（图文编辑：上尉的橄榄绿）

亚瑟·谢尔比乌斯和Enigma

- 转轮机是Vigenere 密码的一种实现。每个转轮是字母的任意组合，有26个位置，并且完成一种简单代替。例如：一个转轮可能被用线连起来以完成用“F”代替“A”，用“U”代替“B”，用“L”代替“C”等等，而转轮的输出端连接到相邻的下一转轮的输入端。
- 例如，在4个转轮的密码机中，第一个转轮可能用“F”代替“A”，第二个转轮可能用“Y”代替“F”，第三个转轮可能用“E”代替“Y”，第四个转轮可能用“C”代替“E”，“C”应该是输出密文。那么当转轮移动后，下一次代替将不同了。
- 为使机器更安全，可以把几个转轮和移动的齿轮结合起来。因为所有转轮以不同的速度移动，n个转轮的机器的周期是26n。为进一步阻止密码分析，有些转轮机在每个转轮上还有不同的位置号。
- 恩尼格玛一般有三个转轮，从五个转轮中选择。转轮机中有一块稍微改变明文序列的插板，有一个反射轮导致每个转轮对每一个明文字母操作两次。

本图中，密码机的四个转子清晰可见。

Enigma
三个转轮的连接示意

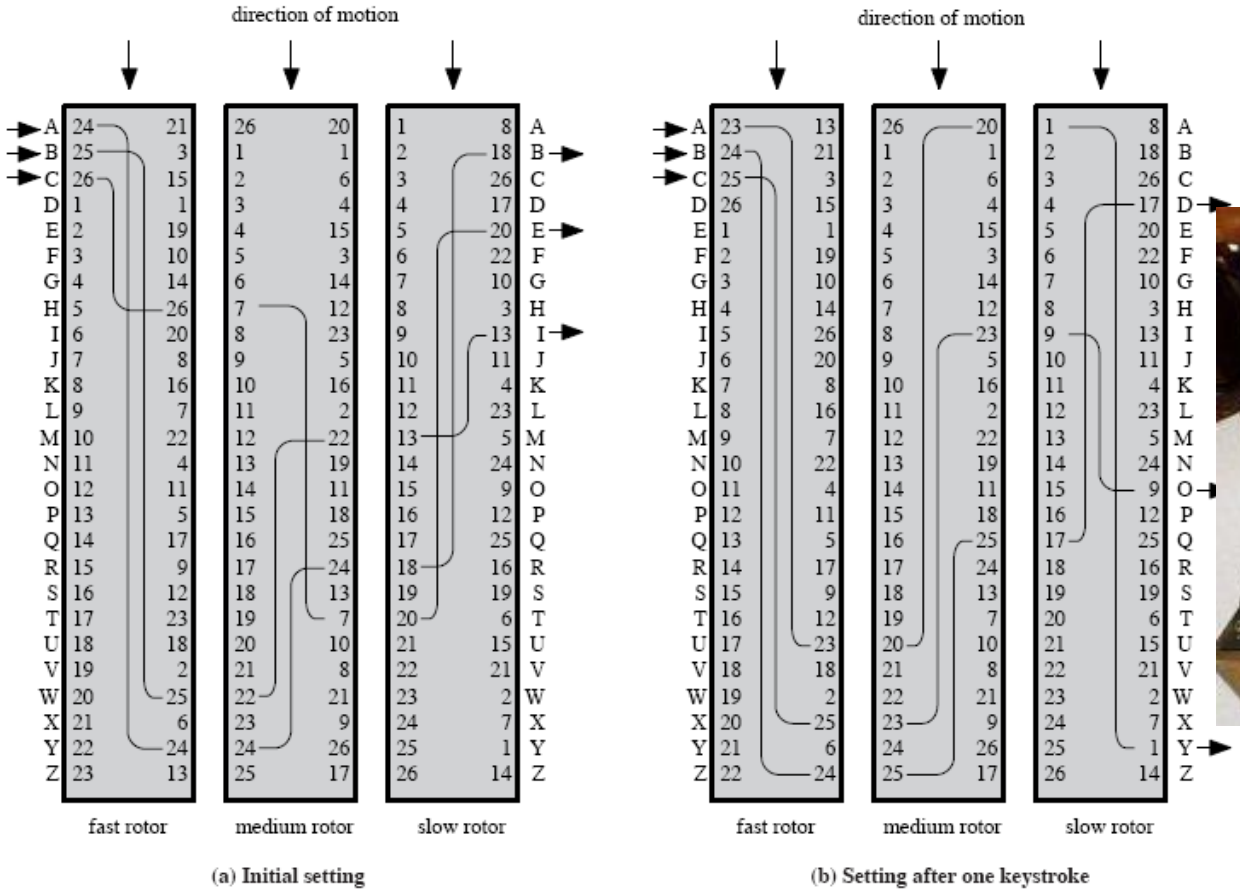


Figure 2.7 Three-Rotor Machine With Wiring Represented by Numbered Contacts

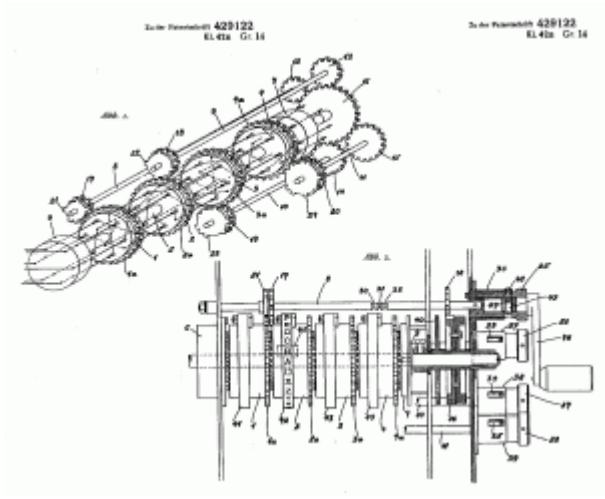
Enigma的使用

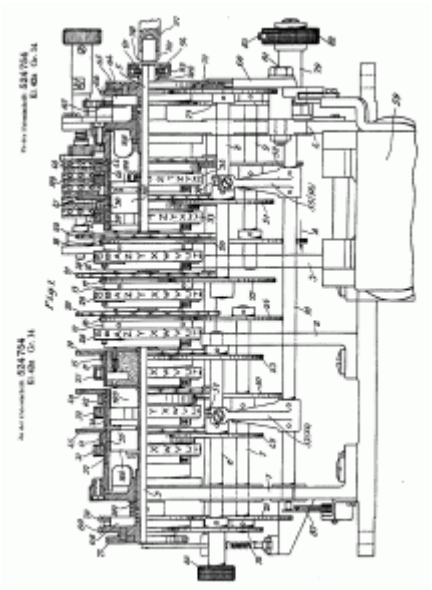
- 使用恩尼格玛通讯时，发信人首先调节三个转子的初始方向，这个转子的初始方向就是密钥，是收发双方预先约定好的。然后依次键入明文，并把显示器上灯泡闪亮的字母依次记下来，最后把记录下的字母按照顺序用正常的电报方式发送出去。
- 收信方收到电文后，只要也使用一台恩尼格玛，按照原来的约定，把转子的方向调整到和发信方相同的初始方向上，然后依次键入收到的密文，显示器上自动闪亮的字母就是明文了。
- 使用恩尼格玛解密和加密的过程完全一样，这就是反射器的作用，同时反射器的一个副作用就是一个字母永远也不会被加密成它自己，因为反射器中一个字母总是被连接到另一个不同的字母。

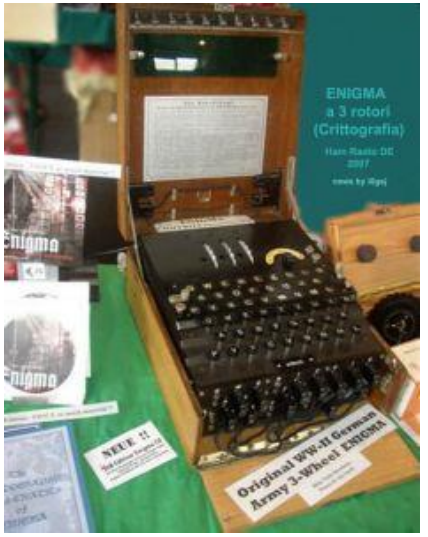
ENIGMA的破解
波兰数学家和密码学家雷耶夫斯基

- 波兰数学家和密码学家马里安·雷耶夫斯基(Marian Adam Rejewski, 1905年8月26日—1980年2月13日)，20世纪30年代领导波兰密码学家率先对德国使用的Enigma密码进行了系统性的研究和破译。雷耶夫斯基首次将严格的数学化方法应用到密码破译领域，这在密码学的历史上是一个重要成就。雷耶夫斯基等人在二战期间破译了大量来自德国的信息，成为整个二战期间盟国破译德军Enigma密码的基础。雷耶夫斯基与波兰数学家杰尔兹·罗佐基和亨里克·佐加尔斯基并称为密码研究领域的“波兰三杰”。
- 2000年7月17日，波兰政府向雷耶夫斯基、罗佐基和佐加尔斯基追授波兰最高勋章。2001年4月21日，雷耶夫斯基、罗佐基和佐加尔斯基纪念基金在波兰华沙设立，基金会在华沙和伦敦设置了纪念波兰数学家的铭牌。

ENIGMA的破解
英国伦敦附近的柏雷屈里庄园密码学校







ENIGMA的破解
计算机科学之父阿兰·图灵

- 阿兰·麦席森·图灵 Alan Mathison Turing(1912年6月23日-1954年6月7日)是英国著名的数学家和逻辑学家，被称为计算机科学之父、人工智能之父，是计算机逻辑的奠基者，提出了“图灵机”和“图灵测试”等重要概念。
- 1936年英国政府在白金汉郡的柏雷屈里庄园设立代码及加密学校(GC&CS ,Government Code and Cipher School)，集结了一大批为破译ENIGMA作出卓越贡献的人们，图灵发明了绰号为“炸弹”(Bombes)的解密机器，被看成一位天才解密分析专家，而于1945年获政府的最高奖—大英帝国荣誉勋章(O.B.E.勋章)。人们认为，通用计算机的概念就是阿兰·麦席森·图灵提出来的
- 战争结束，柏雷屈里庄园被关闭，“炸弹”被拆毁，所有战时有关密码分析和破译的档案资料都被销毁，直到1967年波兰出版第一本关于波兰破译ENIGMA方面的书以及1974年温特伯坦姆写的《超级机密The Ultra Secret》一书出版，人们才知道图灵在解密分析方面的杰出贡献。

计算机科学之父阿兰·图灵

- 在图灵的设计思想指导下，1950年制出了ACE“自动计算机”样机，1958年制成大型ACE机。
- 早在1947年，图灵就提出过自动程序设计的思想，1950年，他提出关于机器思维的问题，他的论文“计算机和智能(Computing machinery and intelligence)引起了广泛的注意和深远的影响。
- 1954年，图灵因食用浸过氰化物溶液的苹果死亡。为了纪念他对计算机科学的巨大贡献，美国计算机协会ACM从1966年起设立一年一度的“图灵奖”，以表彰在计算机科学中做出突出贡献的人。
- 2009年9月10日，在三万民众的联名请愿下，英国当时的首相戈登.布朗正式代表英国政府向图灵因为同性恋被定罪并导致其自杀公开道歉。但英国政府在2012年拒绝了为其追赠死后赦免状的请愿。
- 《The Code Book》作者赛门•辛的链接：www.simonsingh.net
- 破解纳粹的秘密 Decoding Nazi Secrets：http://202.38.64.11/~syang/

Enigma的破解

- 恩尼格玛加密的关键就在于转子的初始方向。当然如果敌人收到了完整的密文，还是可以通过不断试验转动转子方向来找到这个密钥，特别是如果破译者同时使用许多台机器进行这项工作，那么所需要的时间就会大大缩短。对付这样暴力破译法(即一个一个尝试所有可能性的方法)，可以通过增加转子的数量来对付，因为只要每增加一个转子，就能使试验的数量乘上26倍！
- 由于增加转子就会增加机器的体积和成本，恩尼格玛密码机的三个转子是可以拆卸下来并互相交换位置，这样一来初始方向的可能性一下就增加了六倍。假设三个转子的编号为1、2、3，那么它们可以被放成123-132-213-231-312-321这六种不同位置，当然这时收发密文的双方除了要约定转子自身的初始方向，还要约好这六种排列中的一种。

Enigma的破解

- 除了转子方向和排列位置，恩尼格玛还有一道保障安全的关卡，在键盘和第一个转子之间有块连接板。通过这块连接板可以用一根连线把某个字母和另一个字母连接起来，这样这个字母的信号在进入转子之前就会转变为另一个字母的信号。这种连线最多可以有六根，后期的恩尼格玛甚至达到十根连线，这样就可以使6对字母的信号两两互换，其他没有插上连线的字母则保持不变。当然连接板上的连线状况也是收发双方预先约定好的。
- 转子之间的相互位置、转子的初始方向，以及连接板的连线状况组成了恩尼格玛三道牢不可破的保密防线，其中连接板是一个简单替换密码系统，而不停转动的转子，虽然数量不多，但却是点睛之笔，使整个系统变成了复式替换系统。连接板虽然只是简单替换却能使可能性数目大大增加，在转子的复式作用下进一步加强了保密性。

Enigma的破解

- 让我们来算一算经过这样处理，要想通过“暴力破译法”还原明文，需要试验多少种可能性：
  - 三个转子不同的方向组成了26 x 26 x 26＝17576种可能性；
  - 三个转子间不同的相对位置为6种可能性；
  - 连接板上两两交换6对字母的可能性则是异常庞大，有100391791500种；
  - 于是一共有17576 x 6 x 100391791500，其结果大约为10,000,000,000,000,000！即一亿亿种可能性！
- 这样庞大的可能性，即便能动员大量的人力物力，要想靠“暴力破译法”来逐一试验可能性，几乎是不可能的。而收发双方，则只要按照约定的转子方向、位置和连接板连线状况，就可以非常轻松简单地进行通讯了。这就是“恩尼格玛”密码机的保密原理。

解密德军U艇密码机

- 1944年6月4日，美国海军瓜达卡纳尔号航空母舰和5艘驱逐舰组成的编队，在非洲加那利群岛附近海域对德国海军U-505潜艇展开围捕，并缴获了纳粹德国专门用于U艇通讯联系的绝密的密码机恩尼格玛和密码本。从此，德军的U型潜艇完全暴露在盟军的反潜打击之下，德国海军的“狼群”作战遭到彻底失败，并由此改变了整个第二次世界大战的结局。那部对二次大战进程产生过重要影响的德国海军密码机现在存放于美国中央情报局的档案馆。

破解纳粹的Tunny密码

- 柏雷屈里庄园的三位英雄
  - Alan.Turing
  - William. Tutte，数学家，破解了Tunny密码
  - Tommy. Flowers，电气工程师，独立造出了世界上第一台计算机Colossus，用于破解Tunny密码
- 艾森豪威尔说过，Tunny密码的破解，使二战至少缩短了两年

Tunny密码(Lorenz密码)

- Lorenz SZ40密码机
  - 比Enigma复杂得多，但是使用简单，像电传打字机那样直接收发明文
  - 12个转子，用两个密钥进行两次加密
    - 第1轮和第2轮各用5个转子加密
    - 剩下两个转子生成“stutters”，向密钥中添加更多冗余信息
  - 密钥序列为

    23x26x29x31x37x41x43x47x51x53x59x61

    =1,600,000,000,000,000　约1600万亿种不同的组合
- Lorenz密码的弱点
  - 如果两条不同的消息使用相同的密钥加密，那么就有可能将它们还原出来
  - 一个德军发报员使用相同密钥加密两份稍有不同的4000字电文，使得英国人得到了破译的机会

Tunny密码的破译(手工破译)

- 如果两条不同的消息使用相同的密钥加密

{ A+K=N　等式两边相加，消去K，得
{ B+K=P　A+B=N+P, 令G=N+P

现在的问题是有没有办法把G拆分成A和B？

- 数学上是无法做到的，但可以通过常识去猜测可能的答案
  - 把G和A相加，根据电传码表，G和A相加结果是B
  - 例2：RSEZLS是英国两大城市名称之和，假设其中一个是LONDEN，字母相加，得OXFORD
- 天才译码员John Tiltman用10天时间分离出密钥和明文，但是找不到破译所有Tunny密码的适用方法

Tunny密码的破译(数学统计方法)

- William Tuttle的伟大贡献
  - 分析Lorenz密码机的结构，从截获的密电推断密码运作方式，虽然根本没有见过这种密码机
  - 研究出破译这种密码的“1+2”统计学方法(1942年11月发明)，利用数学和统计学来破译密码
- Tommy Flowers的伟大贡献
  - 根据Tuttle提出的数学破译原理制造出第一台半编程型电子计算机Colossus来破译Tunny密码，参与7步破译过程中的2步，其余5步仍由人工完成
  - 该机器能够每秒5000个字符的速度读入截获的电文(5单位电传机纸带)，用电子管电路生成密钥序列，根据Tuttle的数学原理进行破译

致命的一击：美日中途岛海战秘闻

- 日本海军早在1934年就开始发展现代密码体系，从德国购买了一部“恩尼格马”商用密码机并加以改进，造出了自己的密码机，把它发展成为日本整个外交系统广泛使用的战略级密码体制，这一体制被美国军情人员命名为“紫密”(Purple)。
- 1940年8月，英国通信情报处成功破译了“紫密”。其实，“紫密”曾透露日军可能会大规模袭击珍珠港这一极为重大的军事机密，可惜由于种种原因，这一机密在当时并没有引起美国军政要人的重视。
- 此后，日本海军升级了整个密码体系，使用 “舰队密码体制”，高级司令部才能使用的战略级密码，被美国情报人员命名为“JN-25b”。
- 1942年1月20日，日本海军“伊号124”潜艇在澳大利亚海军基地达尔文港外海铺设水雷，遭美国海军驱逐舰以及三艘澳大利亚快艇的围攻，沉没在50米深的海底。美国海军迅速派出熟练的潜水员潜入海底，在伊号124潜艇的残骸里发现了一只保险柜，从中找到一个密码本，表面有铅，遇水后没有溶化。该密码本被交到了夏威夷情报站站长罗彻福特手上，他惊喜地发现，这就是让他头痛不已的日本“JN-25b” 舰队密码体制。而此时，日本海军并不知道“伊号124”潜艇是被击沉的，还以为潜艇沉没是意外事故。因此，一直照旧使用“JN-25b”。

致命的一击：美日中途岛海战秘闻

- 到1942年5月初，JN-25b密 码本已被美国夏威夷情报站还原了1/3，日本人往来的密电有90%的内容都能正确译出。
- 5月20日，罗彻福特截获并破译出日本联合舰队司令下发给各部队的长篇电文，掌握了他们的作战计划。只是在计划中，关于进攻的目标，日军始终用一个代号 “AF”来代替。这个 “AF”究竟是哪里？经过分析罗彻福特认为， “AF”是指中途岛。该岛由周长24公里的环礁组成，陆地面积约5平方公里。距日本2800海里，距夏成夷903海里。美国海军在这里修建了航空和潜艇基地，以使之成为夏威夷群岛的西北屏障。
- 罗彻福特建议太平洋舰队总司令尼米兹通过海底电话，命令中途岛基地用明码报告淡水设备故障，用水困难。还让珍珠港的第 14海军军区煞有介事地回电：已向中途岛派出供水船。日军很快就上钩了，他们用密码通知主力进攻部队携带更多的淡水净化器。这就证明，日军的下一个攻击目标正是中途岛!
- 1942年6月4日清晨，日本攻击机群直扑中途岛。可是，它们所能找到的轰炸目标，只不过是空荡的飞行跑道和几座空机库，岛上所有的飞机此时都已经飞上了高空，那些本应该停在中途岛上的飞机，此时已经在飞往攻击他们舰队的路上。没过多久，美军的32架轰炸机仅用11分钟，就先后击沉了日军的3艘航母 。美军大获全胜，中途岛战役实质上成了太平洋战争的转折点。

2.5 Steganography隐写术

- 隐写术不是加密技术
- 隐写术可以隐藏信息的存在，密码学则通过对文本信息的不同转换而实现信息的不可读
  - 字符标记
  - 不可见墨水
  - 针刺
  - 打字机的色带校正
- 隐写术需要许多额外的开销来隐藏相对较少的信息

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,

Figure 2.8 A Puzzle for Inspector Morse
(from *The Silent World of Nicholas Quinn*, by Colin Dexter)

Summary

- Have considered:
  - classical cipher techniques and terminology
  - monoalphabetic substitution ciphers
  - cryptanalysis using letter frequencies
  - Playfair ciphers
  - polyalphabetic ciphers
  - transposition ciphers
  - product ciphers and rotor machines
  - stenography

复习思考题

1. 对网络安全的攻击主要有哪些？
2. 网络安全服务的目标是什么？
3. 什么是密码？简单加密系统的模型是什么？
4. 什么是理论安全？什么是实际安全？
5. 什么是密码体制？有哪几类密码体制？
6. 现代密码学的基本原则是什么？
7. 加密系统应满足哪些具体要求？