代数模型

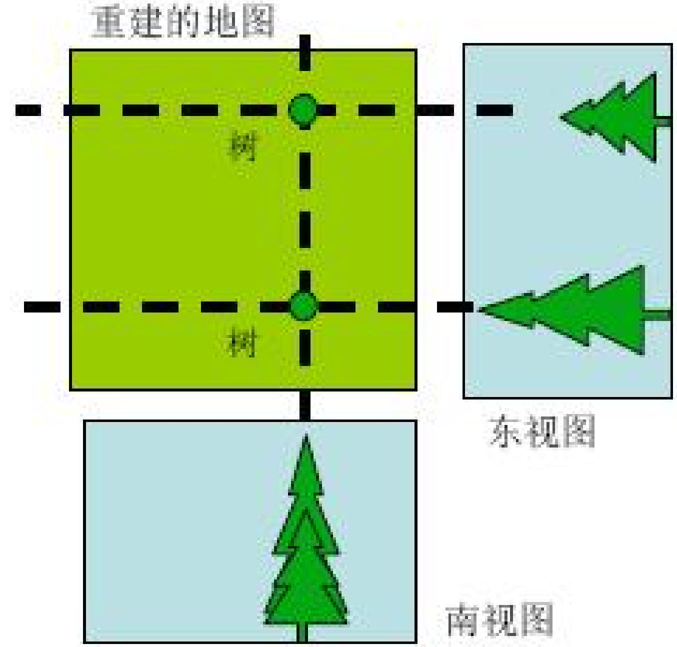
对于工程技术和社会领域的众多问题，当不考虑时间因素的变化（或连续变化），而做为静态问题处理时，我们可以把思维扩展到线性空间，利用线性代数的基本知识建立模型，进而掌握事物的内在规律，预测其发展趋势。这些模型的基本特点是：用相应的向量、矩阵、线性方程等代数模型和手段来刻画和分析实际问题。

任务：体会线性代数的抽象概念怎样运用到解决实际问题的过程中。

断层成像中的基础应用

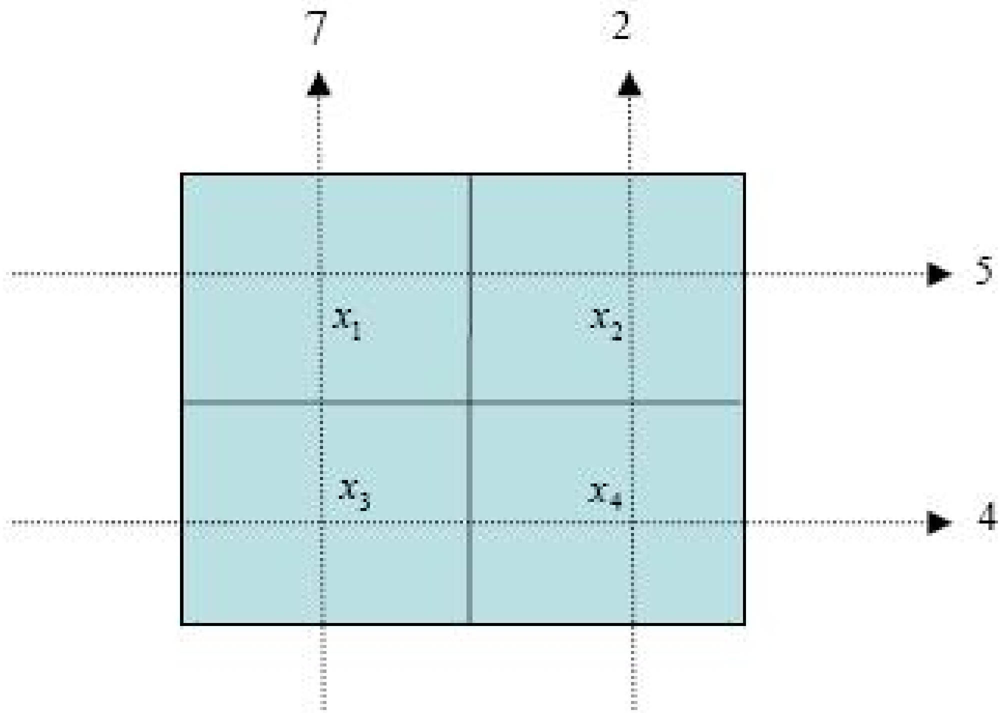
断层成像：获取一个物体内部的截面图像

为了获取西瓜的内部情况，我们只需切开它。
但对一个病人呢？



从不同方向拍到照片：投影（Projection）

用所获取的照片得到整个公园的地图：重建/反投影（Backprojection）



7
2
5
x_1
x_2
x_3
x_4
4

断层成像： 数学计算的手段解决

CT (Computed Tomography 计算机断层成像，直译为计算出的断层成像)

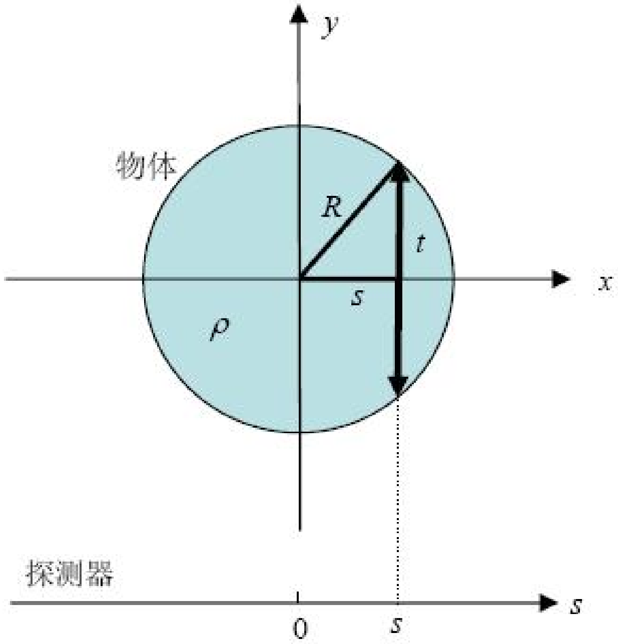
矩阵每一行(列)的求和过程：

图像的射线和(线积分)及投影数据

从物体投影数据得到物体内部断层成像的过程：

图像重建

投影（射线和，线积分）



物体：x-y平面中一个均匀圆盘

圆心：坐标原点

线密度函数：常数ρ

物体的投影值(线积分值)：弦长 t 乘以线密度 ρ

$$p(s)=\begin{cases}\rho t = 2\rho\sqrt{R^2-s^2} & |s|<R \\ 0 & |s|\geq R\end{cases}$$

断层成像问题再复杂一些？

需要更多数据！

如何获取数据?

从多角度采集数据+矩阵求和+数学处理手段

探测器：由四个离散的探测元组成

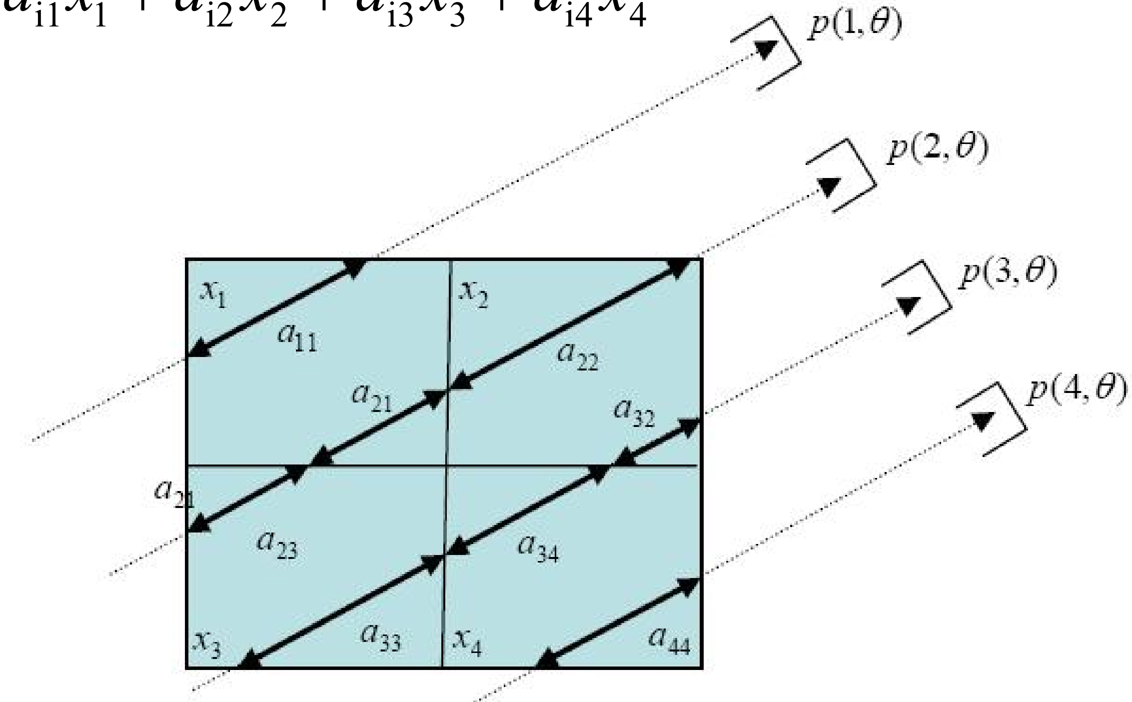
矩阵：连续图像。每个矩阵元素代表一个均匀的像素

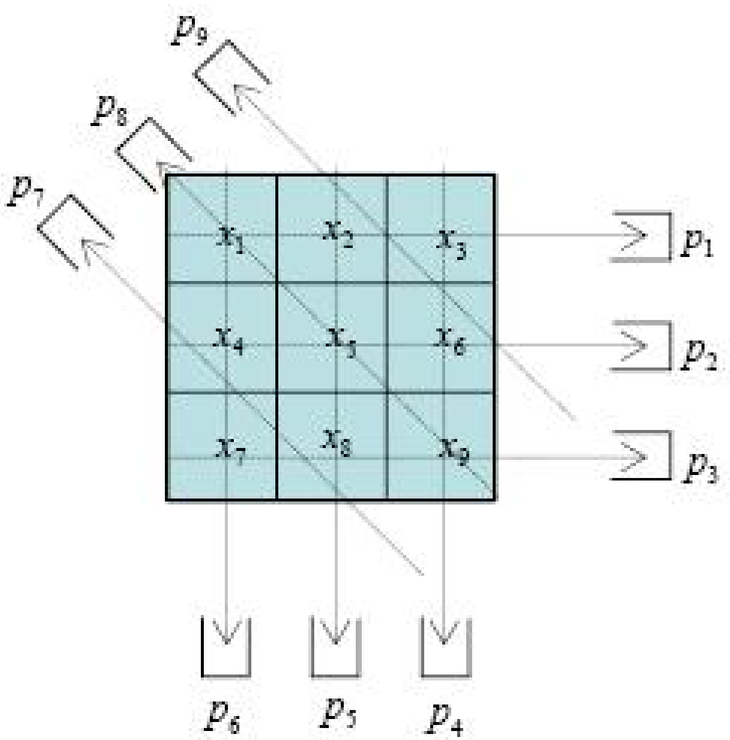
$x_i\ (i=1,2,3,4)$：第i个像素的线密度数值

矩阵图像的投影数据：图像线积分数值 $p(s,\theta)$

线积分的“线”在每个像素内的线段长度a_{ij}(i 是探测元的编号; j 是像素的编号

$$p(i,\theta)=a_{i1}x_1+a_{i2}x_2+a_{i3}x_3+a_{i4}x_4$$

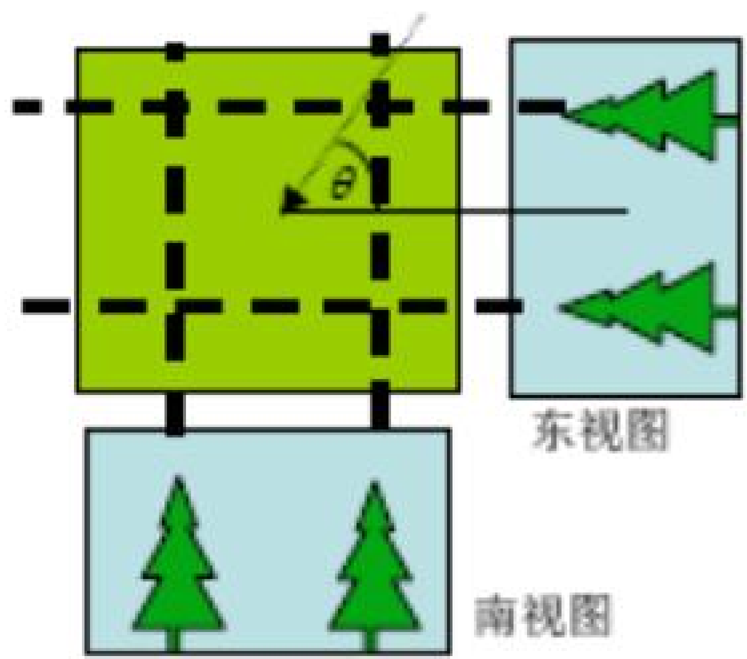




$$
\begin{cases}
x_1 + x_2 + x_3 = p_1 \\
x_4 + x_5 + x_6 = p_2 \\
x_7 + x_8 + x_9 = p_3 \\
x_3 + x_6 + x_9 = p_4 \\
x_2 + x_5 + x_8 = p_5 \\
x_1 + x_4 + x_7 = p_6 \\
2(\sqrt{2}-1)x_4 + 2(\sqrt{2}-1)x_7 + 2(\sqrt{2}-1)x_8 = p_7 \\
\sqrt{2}x_1 + \sqrt{2}x_5 + \sqrt{2}x_9 = p_8 \\
2(\sqrt{2}-1)x_2 + (2-\sqrt{2})x_3 + 2(\sqrt{2}-1)x_6 = p_9
\end{cases}
$$

图像重建问题：解线性方程组，求解x

思考：如图所示，在那两张照片中都可以看到两棵不重叠的大树。你可以唯一地画出那两棵树的地图吗？若不行的话，你也许需要多照些照片。如果你只允许再多照一张照片，选个什么角度照呢？

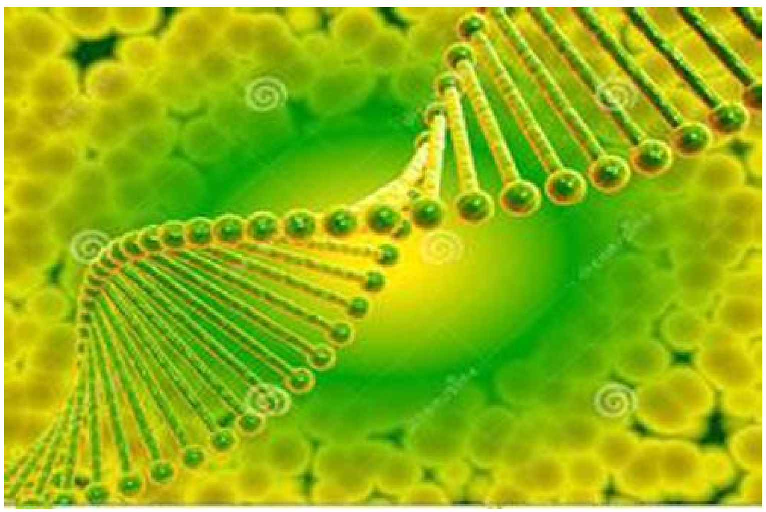


植物基因的分布

设一农业研究所植物园中某种植物的基因型为AA、Aa和aa。研究所计划采用AA型的植物与每一种基因型植物相结合的方案培育植物后代。问经过若干年后，这种植物的任意一代的三种基因型分布如何?

目的：研究能指导植物性状（如抗病抗虫、抗逆等）的基因培育方式，最终达到改变以及培育植物新品种的目的。

- 基因对确定了植物的特征
- 在常染色体的遗传中，后代是从每个亲本的基因对中各继承一个基因，形成自己的基因对(基因型)



育种方式：

AA型　　　其它基因型

后代

在我们所研究的问题中，植物的基因对为AA、Aa、aa这3种

记：

$x_1(n)$—第n代中基因型AA的植物占植物总数的百分比

$x_2(n)$—第n代中基因型Aa的植物占植物总数的百分比

$x_3(n)$—第n代中基因型aa的植物占植物总数的百分比

显然

$$x_1(n)+x_2(n)+x_3(n)=1$$

相邻两代间基因转移关系：

	概率	父体-母体的基因对		
		AA-AA	AA-Aa	AA-aa
后代基因对	AA	1	1/2	0
	Aa	0	1/2	1
	aa	0	0	0

育种方式：

AA型　　其它基因型

$\searrow$ $\swarrow$

后代

相邻两代间基因转移关系：

	概率	父体-母体的基因对		
		AA-AA	AA-Aa	AA-aa
后代基因对	AA	1	1/2	0
	Aa	0	1/2	1
	aa	0	0	0

故第n代与n-1代植物的基因型分布的关系为：

$$x_1(n) = x_1(n-1) + \frac{1}{2}x_2(n-1)$$

$$x_2(n) = \frac{1}{2}x_2(n-1) + x_3(n-1)$$

$$x_3(n) = 0,$$

引入 $L=\begin{pmatrix} 1 & \frac{1}{2} & 0 \\ 0 & \frac{1}{2} & 1 \\ 0 & 0 & 0 \end{pmatrix}$, $\vec{x}(n)=\begin{pmatrix} x_1(n) \\ x_2(n) \\ x_3(n) \end{pmatrix}$

则第n代与n-1代植物的基因型分布的关系的向量形式为:

$$\vec{x}(n)=L\vec{x}(n-1), \qquad n=1,2,\ldots \qquad (1)$$

由（1）解得:

$$\vec{x}(n)=L^n\vec{x}(0), \qquad n=1,2,\ldots \qquad (2)$$

L^n 的计算：

利用线性代数中**对角化的方法**将L对角化, 即求出可逆矩阵P 和对角矩阵D, 使得

$$L = PDP^{-1}$$

从而有

$$L^n = PD^nP^{-1}$$

利用特征值和特征向量的方法求得

$$D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{2} & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad P = P^{-1} = \begin{pmatrix} 1 & 1 & 1 \\ 0 & -1 & -2 \\ 0 & 0 & 1 \end{pmatrix}$$

从而得

$$L^n = \begin{pmatrix} 1 & 1-\left(\frac{1}{2}\right)^n & 1-\left(\frac{1}{2}\right)^{n-1} \\ 0 & \left(\frac{1}{2}\right)^n & \left(\frac{1}{2}\right)^{n-1} \\ 0 & 0 & 0 \\ & & \end{pmatrix}$$

将L^n代入(2)得

$$x_1(n)=x_1(0)+\left(1-\left(\frac{1}{2}\right)^n\right)x_2(0)+\left(1-\left(\frac{1}{2}\right)^{n-1}\right)x_3(0)$$

$$x_2(n)=\left(\frac{1}{2}\right)^n x_2(0)+\left(\frac{1}{2}\right)^{n-1} x_3(0)$$

$$x_3(n)=0$$

显然可以看出当

$$n\to\infty\text{时，}\ x_1(n)\to 1, x_2(n)\to 0, x_3(n)\to 0$$

结论： 培育得植物AA型基因所占的比例在不断增加，**在极限状态下所有植物的基因型都会是AA型**。

信息的加密与解密

信息安全本身包括的范围很大，大到国家军事政治等机密安全，小范围的当然还包括如防范商业企业机密泄露，个人信息的泄露等。网络环境下的信息安全体系是保证信息安全的关键，包括计算机安全操作系统、各种安全协议、安全机制（数字签名，信息认证，数据加密等），直至安全系统，其中任何一个安全漏洞便可以威胁全局安全。

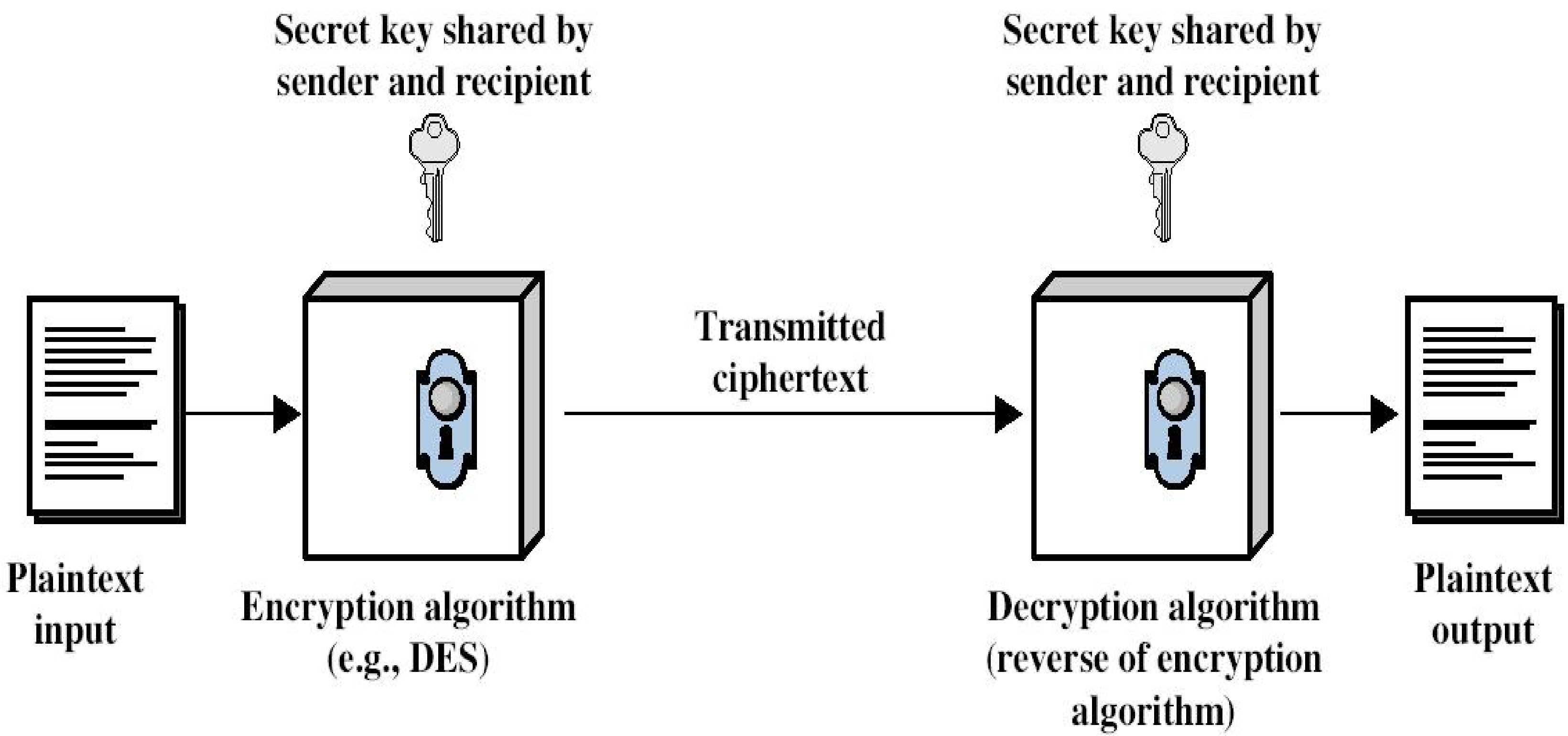
信息安全服务至少应该包括支持信息网络安全服务的基本理论，以及基于新一代信息网络体系结构的网络安全服务体系结构。

- 密码的设计和使用至少可从追溯到四千多年前的埃及、巴比伦、罗马和希腊，历史极为久远
- 古代隐藏信息的方法主要有两大类：其一为隐藏信息载体，采用隐写术等；其二为变换信息载体，使之无法为一般人所理解

简单定义

在密码学中，信息代码被称为密码，加密前的信息被称为明文，经加密后不为常人所理解的用密码表示的信息被称为密文(ciphertext)，将明文转变成密文的过程被称为加密(enciphering)，其逆过程则被称为解密(deciphering)，而用以加密、解密的方法或算法则被称为密码体制(crytosystem)。

常规加密简化模型



Secret key shared by
sender and recipient
Secret key shared by
sender and recipient
Transmitted
ciphertext
Plaintext
input
Encryption algorithm
(e.g., DES)
Decryption algorithm
(reverse of encryption
algorithm)
Plaintext
output

记全体明文组成的集合 为U，全体密文组成的集合 为V，称U为明文空间，V为密文空间。加密常利用某一被称为密钥的东西来实现，它通常取自于一个被称为密钥空间的含有若干参数的集合K。按数学的观点来看，加密与解密均可被看成是一种变换：取一$k \in K$，　$u \in U$，令 $u \xrightarrow{k} v \in V$，$v$为明文$u$在密钥$K$下的密文，而解码则要用 到$K$的逆变换$K^{-1}$，。由此可见，密码体系虽然可以千姿百态，但其关键还在于密钥的选取。

早在4000多年前，古希腊人就用一种名叫“天书”的器械来加密消息。该密码器械是用一条窄长的纸带缠绕在一个直径确定的圆筒上，明文逐行横写在纸带上，当取下纸带时，字母的次序就被打乱了，消息得以隐蔽。收方阅读消息时，要将纸带重新绕在直径与原来相同的圆筒上，才能看到正确的消息。在这里圆筒的直径起到了密钥的作用。

随着计算机与网络技术的迅猛发展，大量各具特色的密码体系不断涌现。离散数学、数论、计算复杂性、混沌、……，许多相当高深的数学知识都被用上，逐步形成了（并仍在迅速发展的）具有广泛应用面的现代密码学 。

在科学上,如果一个系统的演变过程对初态非常敏感,人们就称它为混沌系统。

*混沌*系统具有良好的伪随机特性、轨道的不可预测性、对初始状态及控制参数的敏感性等一系列特性，这些特性与*密码*学的很多要求是吻合的。

移位密码体制

移位密码采用移位法进行加密，明文中的字母重新排列，本身不变，只是位置改变了。

一种移位法是采用将字母表中的字母平移若干位的方法来构造密文字母表，传说这类方法是由古罗马皇帝凯撒最早使用的，故这种密文字母表被称为凯撒字母表。例如，如用将字母表向右平移3位的方法来构造密文字母表，可得：

明文字母表： ABCDEFGHIJKLMNOPQRSTUVWXYZ

密文字母表： DEFGHIJKLMNOPQRTSUVWXYZABC

因此 “THANK YOU” ⟶ “WKDQN BRX”

以上移位较易被人破译，为打破字母表中原有的顺序还可采用所谓路线加密法，即把明文字母表按某种既定的顺序安排在一个矩阵中，然后用另一种顺序选出矩阵中的字母来产生密文表。

例如，对明文：**THE HISTORY OF ZJU IS MORE THAN ONE HUNDRED YEARS**.以7列矩阵表示如下：

THEHIST
ORYOFZJ
UISMORE
THANONE
HUNDRED
YEARS

再按事先约定的方式选出密文。例如，如按列选出，得到密文：**touthyhrihueeysanahomndrifoorsszrnetjeed**

- 使用不同的顺序进行编写和选择，可以得到各种不同的路线加密体制。对于同一明文消息矩阵，采用不同的抄写方式，得到的密文也是不同的。

- 当明文超过规定矩阵的大小时，可以另加一矩阵。当需要加密的字母数小于矩阵大小时，可以在矩阵中留空位或以无用的字母来填满矩阵。

移位法密码的破译

对窃听到的密文进行分析时，穷举法和统计法是最基本的破译方法。

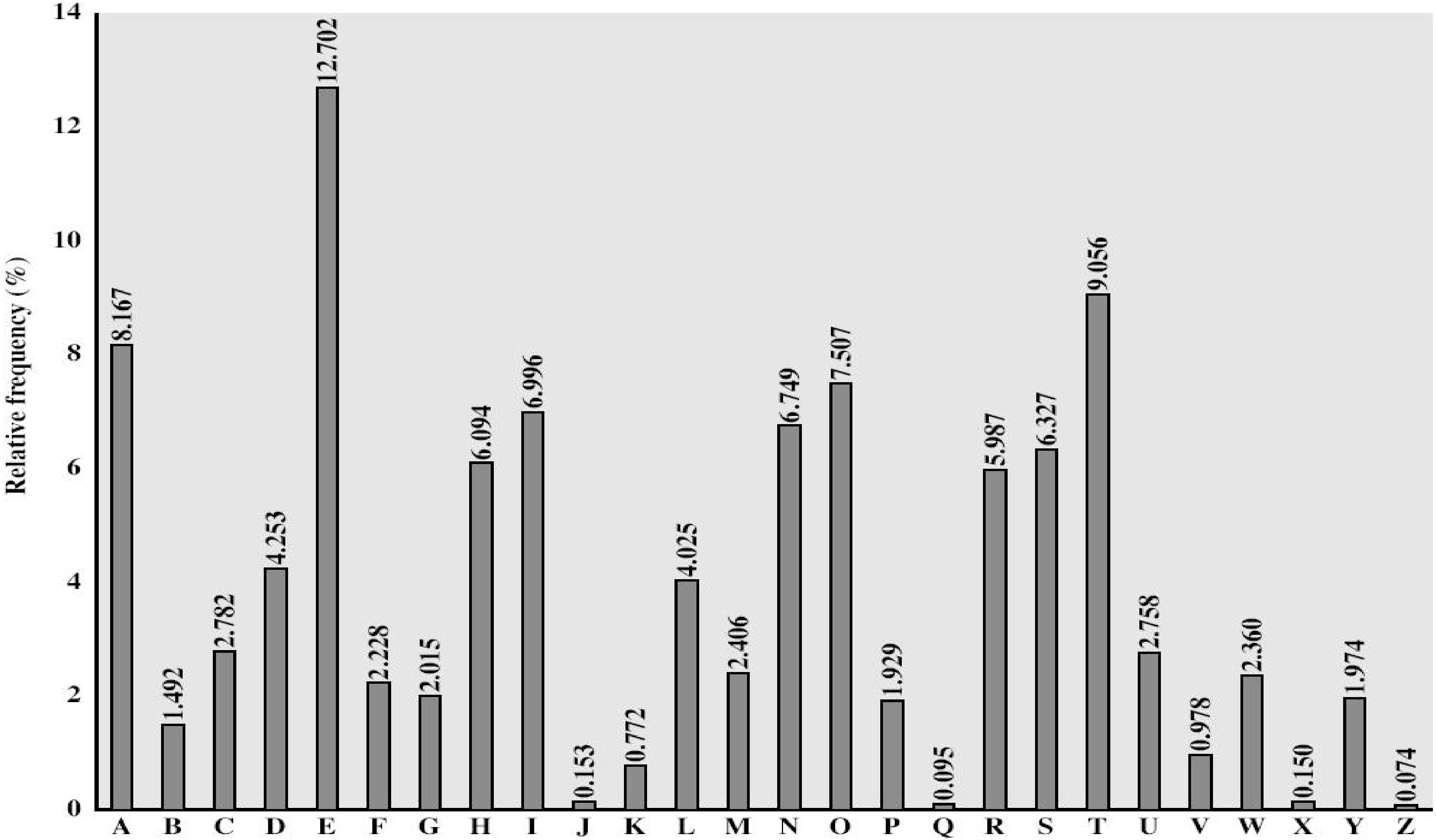
穷举分析法 就是对所有可能的密钥或明文进行逐一试探，直至试探到“正确”的为止。此方法需要事先知道密码体制或加密算法（但不知道密钥或加密具体办法）。破译时需将猜测到的明文和选定的密钥输入给算法，产生密文，再将该密文与窃听来的密文比较。如果相同，则认为该密钥就是所要求的，否则继续试探，直至破译。以英文字母为例，当已知对方在采用代替法加密时，如果使用穷举字母表来破译，那么对于最简单的一种使用单字母表一单字母一单元代替法加密的密码，字母表的可能情况　有**26！**种，可见，单纯地使用穷举法，在实际应用中几乎是行不通的，只能与其它方法结合使用。

统计法是根据统计资料进行猜测的。在一段足够长且非特别专门化的文章中，字母的使用频率是比较稳定的。在某些技术性或专门化文章中的字母使用频率可能有微小变化。

在上述两种加密方法中字母表中的字母是一一对应的，因此，在截获的密文中各字母出现的概率提供了重要的密钥信息。根据权威资料报道，可以 将26个英文字母按其出现的频率大小较合理地分为五组：

I. t,a,o,i,n,s,h,r;
II. e;
III. d,l;
IV. c,u,m,w,f,g,y,p,b;
V. v,k,j,x,q,z;

不仅单个字母以相当稳定的频率出现，相邻字母对和三字母对同样如此。



Relative Frequency of Letters in English Text

按频率大小 将双字母排列如下：

th,he,in,er,an,re,ed,on,es,st,en,at,to,nt,ha,nd,ou,ea,ng,as,or,ti,is,er,it,ar,te,se,hi,of

使用最多的三字母按频率大小排列如下：

The,ing,and,her,ere,en a,nth,was,eth,for,dth

下面介绍一下统计观察的三个结果：

a)单词the在这些统计中有重要的作用；

b)以e，s，d，t为结尾的英语单词超过了一半；

c)以t，a，s，w为起始字母的英语单词约为一半。

对于a)，如果 将the从明文中删除，那 么t的频率将要降到第二组中其他字母之后， 而h将降到第三组中，并且th和he就不再是最众多的字母了。

以上对英语统计的讨论是在仅涉 及26个字母的假设条件下进行的。实际上消息的构成还包括间隔、标点、数字等字符。总之，破译密码并不是件很容易的事。

希尔密码

移位密码的一个致命弱点是明文字符和密文字符有相同的使用频率,破译者可从统计出来的字符频率中找到规律，进而找出破译的突破口。要克服这一缺陷，提高保密程度就必须改变字符间的一一对应。

1929年，希尔利用线性代数中的矩阵运算，打破了字符间的对应关系，设计了一种被称为希尔密码的代数密码。为了便于计算，希尔首先将字符变换成数，例如，对英文字母，我们可以作如下变换：

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
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0

将明文分成 **n**个一组，用对应的数字代替，就变成了一个**n**维向量。如果取定一 个**n**阶的非奇异矩 阵**A**（此矩阵为主要密钥），用**A**去乘每一向量，即可起到加密的效果，解密也不麻烦，将密文也分 成**n**个一组，同样变换 成**n**维向量，只需用**A**逆去乘这些向量，即可将他们变回原先的明文。

但在具体实施时，我们很快会发现一些困难：

首先，我们的英文字母是与0～25这26个整数1-1对应的，所以变换或逆变换后需要产生0～25之间的整数。

只要密钥矩阵A或其逆矩阵A^{-1}是非负整数矩阵，以A或A^{-1}乘以任一向量后所得结果仍为整向量，对该整向量的每个元素以26为模求同余运算即可使密文或解密后的密文为0～25之间的整数。

第一个困难引入同余运算即可解决

其次，A^{-1}也应该是0～25之间的整数矩阵。这就要对密钥矩阵的行列式det(A)增加了一些限制。

由 线性代数可知 $A^{-1}=\dfrac{A^*}{\det(A)}$, 其中$A^*$是A的伴随矩阵，从而$A^{-1}$的元素中就有可能出现分数。克服这一困难的途径仍然是引入同余运算，即在同余意义上引入除法：

若$a\geq 0, b\geq 0$, 满足 $ab(\bmod 26)=1$,则称b为a在同余意义上的逆元，记作$a^{-1}=b(\bmod 26)$

与逆矩阵的定义类似

故若有$\det(A)^{-1}=b_0(\bmod 26)$，则 $A^{-1}=b_0A^*$.

一个矩阵要成为密钥矩阵，它的行列式必须有逆元

关于0～25之间的整数有无同余意义上的逆元有下面的定理：

定理1 $a\in\{0,...,25\}$，若 $\exists a^{-1}\in\{0,25\}$ 使得 $aa^{-1}=a^{-1}a\equiv 1(\bmod 26)$，则必有 $\gcd\{a,26\}=1$，其中$\gcd\{a,26\}$为 a 与26的最大公因子。

还可以证明，如果a^{-1}存在，那么它是唯一的。由定理1，0～25中除13以外的奇数均可取作这里的a，它们的逆元如下表。

a	1	3	5	7	9	11	15	17	19	21	23	25
a^{-1}	1	9	21	15	3	19	7	23	11	5	17	25

Hill密码的加密过程

- 选择一个n阶可逆矩阵A作为加密矩阵；
- 将明文字符按顺序排列分组；
- 将明文字符对应一个整数，组成一组列向量；
- 用加密矩阵左乘每一列向量；
- 将新向量的每个分量关于模m取余运算；
- 将新向量的每个整数对应于一个字符。

解密过程相反。

例　取A = 3用希尔密码体系加密语句
THANK YOU

步1　将THANK YOU转换成
（20，8，1，14，11，25，15，21）

步2　每一分量乘以 A并关于26取余得
（8，24，3，16，7，23，19，11）

密文为HXCPG WSK

现在我们已不难将方法推 广到n为一般整数的情况了,只需在乘法运算中结合应用取余，求逆矩阵时用逆元素相乘来代替除法即可。

例　取$A=\begin{bmatrix}1 & 2\\0 & 3\end{bmatrix}$则 $A^{-1}=\begin{bmatrix}1 & 8\\0 & 9\end{bmatrix}$ (具体求法见后),用A加密THANK YOU,再用A^{-1}对密文解密

解:(希尔密码加密)用相应数字代替字符，划分为两个元素一组并表示为向量:

$$\begin{bmatrix}20\\8\end{bmatrix}\begin{bmatrix}1\\14\end{bmatrix}\begin{bmatrix}11\\25\end{bmatrix}\begin{bmatrix}15\\21\end{bmatrix}$$

用矩阵A左乘各向量加密（关 于26取余）得

$$\begin{bmatrix}10\\24\end{bmatrix}\begin{bmatrix}3\\16\end{bmatrix}\begin{bmatrix}9\\23\end{bmatrix}\begin{bmatrix}5\\11\end{bmatrix}$$

得到密文　JXCPI WEK

（希尔密码解密）

用A^{-1}左乘求得的向量，即可还原为原来的向量。希尔密码是以矩阵 法为基础的，明文与密文的对应由n阶矩阵A确定。矩阵A的阶数是事先约定的，与明文分组时每组字母的字母数量相同，如果明文所含字数与n不匹配，则最后几个分量可任意补足。

A^{-1}的求法

方法1 利用公式 $A^{-1}=\frac{A^*}{\det(A)}$ ，例如，若取 $A=\begin{bmatrix}1 & 2\\ 0 & 3\end{bmatrix}$ ，

则 $\det(A)=3$ ，$\frac{1}{\det(A)}=9$ ，$A^{-1}\equiv 9\begin{bmatrix}3 & -2\\ 0 & 1\end{bmatrix}$ (mod26)，即

$$A^{-1}=\begin{bmatrix}1 & 8\\ 0 & 9\end{bmatrix}$$

方法2 利用高斯消去法。将矩阵(A, E)中的矩阵A消为E，则原先的E即被消成了A^{-1}，

如

$$\left(\begin{bmatrix}1 & 2\\0 & 3\end{bmatrix},\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}\right)\rightarrow$$ (用**9**乘第二行并取同 余) $$\rightarrow\left(\begin{bmatrix}1 & 2\\0 & 1\end{bmatrix},\begin{bmatrix}1 & 0\\0 & 9\end{bmatrix}\right)$$

第一行减去第二行 的**2**倍并取同余，得

$$\left(\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix},\begin{bmatrix}1 & 8\\0 & 9\end{bmatrix}\right)$$

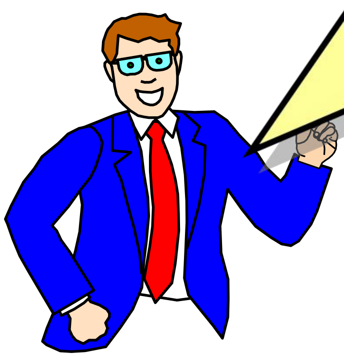
左端矩阵已化为单位阵，故右端矩阵即为 A^{-1}

（希尔密码的破译）

希尔密码体系为破译者设置了多道关口，加大了破译难度。破译和解密是两个不同的概念，虽然两者同样是希望对密文加以处理而得 …… 同——破译密码时，…… 一方需要依据密 …… 等等各方面的信息 …… 重要的是“猜测” …… 破译的结果。破译希 …… 、所对应的字母表 …… 矩阵A。

由线性代数的知识可以知道，矩阵完全由一组基的变换决定，对于n阶矩阵A，只要猜出密文中n个线性无关的向量 $(i=1, 2, \ldots, n)$

对应的明文 $(i=1, 2, \ldots, n)$是什么，即可确定A，并将密码破译。



在实际计算中，可以利用以下方法：

令 $P=(p_1,p_2,\ldots,p_n)^T$，$Q^T=A(p_1,p_2,\ldots,p_n)=AP^T$

则

$$Q=PA^T,P=Q(A^T)^{-1}$$

取矩阵[Q | P],经过一系列初等行变换，将由密文决定的n维矩阵Q化为n阶单位阵 I的时候，由明文决定的矩阵P自动化为 $(A^{-1})^T$，即 ：

$$[Q,P]=[Q,Q(A^T)^{-1}]\longrightarrow(\text{初等行变换})$$

$$\longrightarrow[Q^{-1}Q,Q^{-1}Q(A^T)^{-1}]=[I,(A^T)^{-1}]$$