第2章 Shannon理论

杨礼珍

同济大学计算机科学与技术系, 2017

Outline

第2章 Shannon理论

本章作业

第2章习题2.3

1949年，Shannon在《Bell Systems Technical Journal》上发表的论文“Communication Theory of Secrecy System”使通信保密由艺术变成科学。
本章将学习Shannon的三点思想：

- 无条件安全的密码体制的数学定义：完善保密性，以及完善保密的密码体制。（学习重点）
- 唯密文攻击需要的最短密文长度：惟一解距离，及惟一解距离估计。（理解其结论对密码学的意义）
- 私钥密码体制（即加密密钥和解密密钥都必须保密的）的设计方法：乘积密码。（理解其结论对密码学的意义）

密码学由艺术成为科学的第一步是弄清楚什么是安全，才能讨论如何设计安全的密码体制。

定义密码体制的安全性的要素：

- 敌手模型：
  - 攻击模型(敌手知道的信息): 唯密文分析，已知明文分析，选择明文分析，选择密文分析。
  - 敌手的计算能力
    - 有限计算能力：
    - 无限计算能力： 对攻击者Oscar的计算量没有限制，此时定义的密码体制称为无条件安全的。
- 成功分析的定义：成功分析与敌手模型、明文概率分布、密钥概率分布有关，以概率描述。

可证明安全性：通过归约的方式为安全性提供证据。如：

- 在某些假设下，证明密码体制满足所定义的安全性。
- 在无假设下，证明密码体制满足所定义的安全性

Shannon定义的密码体制的安全性—完善保密性：

- 敌手模型：
  - 攻击模型：唯密文攻击
  - 敌手计算能力：无限计算能力
- 假定一个特定的密钥$K \in \mathcal{K}$只用于一次加密，即加密一次后，下一次加密重新选择密钥。
- 成功分析的定义：即如果对于任意的$x \in \mathcal{P}$和$y \in \mathcal{C}$，都有

$$Pr[x|y] = Pr[x]$$

也就是说，给定密文y，明文x的后验概率等于明文x的先验概率。

符号说明：设X为随机变量，$Pr[x]$为$Pr[X = x]$的简写。

下面将证明，以下密码体制是完善保密的：

- 移位密码具有完善保密性。
- 定理2.4条件下的密码体制是完善保密的
- 一次一密密码体制满足定理2.4，是完善保密的。

证明Shannon的安全理论需要用到的概率论基础回顾：

定理2.1（Bayes定理） 如果$Pr[y] > 0$，那么：

$$Pr[x|y] = \frac{Pr[x]Pr[y|x]}{Pr[y]}$$

推论2.2 X和Y是统计独立的随机变量，当且仅当对所有的$x \in X$和$y \in Y$，都有$Pr[x|y] = Pr[x]$。

完善保密性充分性证明的思路：

$$Pr[\mathbf{Y}=y|\mathbf{X}=x]=Pr[\{K:x=d_K(y)\}]=\sum_{\{K:x=d_K(y)\}}Pr[\mathbf{K}=K] \quad (1)$$

$$Pr[\mathbf{Y}=y|\mathbf{K}=K]=Pr[\mathbf{X}=d_K(y)]$$

那么由全概率公式得到：

$$Pr[\mathbf{Y}=y] = \sum_{\{K\in\mathcal{K}\}}Pr[\mathbf{K}=K]Pr[\mathbf{Y}=y|\mathbf{K}=K] \quad (2)$$

$$= \sum_{\{K\in\mathcal{K}\}}Pr[\mathbf{K}=K]Pr[\mathbf{X}=d_K(y)] \quad (3)$$

把上面式子代入Bayes公式$Pr[x|y]=\frac{Pr[x]Pr[y|x]}{Pr[y]}$。

定理2.3

假设移位密码的26个密钥都是以相同的概率1/26使用的，则对于任意的明文概率分布，移位密码具有完善保密性。

说明：

- 以上定理说明如果移位密码的密钥只是用于一次加密，那么是“不可攻破的”，和攻击者的拥有的计算资源无关。
- 密钥只用于一次加密，不等于相同的密钥K只用于一次加密中，可能在后面的加密中仍然会使用密钥K，但是每次加密选择的密钥都是统计独立的，而且每个取值的概率均等。

证明：

$$
\begin{aligned}
Pr[\mathbf{Y}=y] &= \sum_{K\in\mathbb{Z}_{26}} Pr[\mathbf{K}=K]Pr[\mathbf{X}=d_K(y)] \text{(由公式(3))} \\
&= \sum_{K\in\mathbb{Z}_{26}} \frac{1}{26} Pr[\mathbf{X}=y-K] \Longleftarrow Pr[K]=\frac{1}{26}, d_K(y)=y-K \\
&= \frac{1}{26}\sum_{K\in\mathbb{Z}_{26}} Pr[\mathbf{X}=y-K] \\
&= \frac{1}{26}\cdot 1 \Longleftarrow \text{因为} y-K(K=0,\ldots,25)\text{正好取尽} \\
&= \frac{1}{26} \qquad\qquad 0,\ldots,25\text{上的每个值一次}
\end{aligned}
$$

$$\begin{aligned} Pr[y|x] &= Pr[\mathbf{K} = (y - x) \bmod 26] \Longleftarrow y = (x + K) \bmod 26 \\ &= \frac{1}{26} \end{aligned}$$

应用Bayes公式，计算得到：

$$\begin{aligned} Pr[x|y] &= \frac{Pr[x]Pr[y|x]}{Pr[y]} \\ &= \frac{Pr[x]\frac{1}{26}}{\frac{1}{26}} \\ &= Pr[x] \end{aligned}$$

因此证明了移位密码是完善保密性的。
练习：习题2.3，使用定理2.3中同样的思路，把$P(x|y)$写成$P(x)$和$P(k)$的表达式。

完善保密性的2个必要条件： 假设$Pr[y] > 0$（这个假设是合理的，因为如果$Pr[y] = 0$，我们可以把它从密文空间$\mathcal{C}$中去掉），必有

- $|\mathcal{K}| \geq |\mathcal{C}|$：由Bayes定理，对于任意$x \in \mathcal{P}, y \in \mathcal{C}$有：

$$Pr[x|y] = Pr[x] \Longleftrightarrow Pr[y|x] = Pr[y]$$

对固定的明文x，$Pr[y|x] = Pr[y] > 0$说明对于每个$y \in \mathcal{C}$，一定至少存在一个密钥K满足$e_K(x) = y$，并且对不同的$y_1 \neq y_2$，若$e_{K_1}(x) = y_1$，$e_{K_2}(x) = y_2$，那么必有$K_1 \neq K_2$(若不然x被同一密钥加密成不同的密文)，因此有$|\mathcal{K}| \geq |\mathcal{C}|$。

- $|\mathcal{C}| \geq |\mathcal{P}|$：对同一密钥，每个明文被加密成不同的密文，因此$|\mathcal{C}| \geq |\mathcal{P}|$。

定理2.4

假设密码体制$(\mathcal{P},\mathcal{C},\mathcal{K},\mathcal{E},\mathcal{D})$满足$|\mathcal{K}|=|\mathcal{C}|=|\mathcal{P}|$。这个密码体制是完善保密的，当且仅当每个密钥被使用的概率都是$1/|\mathcal{K}|$，并且对于任意的$x\in\mathcal{P}$和$y\in\mathcal{C}$，存在唯一的密钥$\mathcal{K}$使得$e_K(x)=y$。

说明：

- 移位密码是定理2.4的特殊情形。
- 定理2.4的另一个著名例子是“一次一密”密码体制。
- 完善保密的更一般的充分必要条件由第2章习题2.11给出：密码体制是完善保密的当且仅当$H(\mathbf{P}|\mathbf{C})=H(\mathbf{P})$。

证明：（1）首先证明必要性。假设密码体制是完善保密性的。由前面讨论知道

$$Pr[x|y] = Pr[x] \Longleftrightarrow Pr[y|x] = Pr[y] > 0$$

这说明对任意$x \in \mathcal{P}$和$y \in \mathcal{C}$，一定至少存在一个密钥K满足$e_K(x) = y$，否则会有$Pr[y|x] = 0$，因此会有不等式：

$$|\mathcal{C}| = |e_K(x) : K \in \mathcal{K}| \leq |\mathcal{K}|(\text{这里}x\text{是固定的})$$

而我们假设$|\mathcal{C}| = |\mathcal{K}|$，那么：

$$|e_K(x) : K \in \mathcal{K}| = |\mathcal{K}|$$

这说明，不存在两个不同的密钥K_1和K_2，使得$e_{K_1}(x) = e_{K_2}(x) = y$。因此对于$x \in \mathcal{P}$和$y \in \mathcal{C}$，刚好存在一个密钥$K$使得$e_K(x) = y$。

证明续：记$n = |\mathcal{K}|$。设$\mathcal{P} = \{x_i : 1 \leq i \leq n\}$并且固定一个密文$y \in \mathcal{C}$。设密钥为$K_1, K_2, \ldots, K_n$，并且$e_{K_i}(x_i) = y, 1 \leq i \leq n$。我们有

$$\begin{aligned} Pr[K_i] &= Pr[y|x_i] \\ &= Pr[y] \end{aligned}$$

所以$Pr[K_i] = \frac{1}{|K|}$。

(2)充分性。和定理2.3证明类似。

密码体制2.1（一次一密）

假设$n \geq 1$是正整数，$\mathcal{P} = \mathcal{C} = \mathcal{K} = (\mathbb{Z}_2)^n$。
对$x = (x_1, x_2, \ldots, x_n)$，$K = (K_1, K_2, \ldots, K_n)$，定义

$$e_K(x) = (x_1 \oplus K_1, x_2 \oplus K_2, \ldots, x_n \oplus K_n)$$

解密和加密是一样的，如果$y = (y_1, y_2, \ldots, y_n)$，那么

$$d_K(y) = (y_1 \oplus K_1, y_2 \oplus K_2, \ldots, y_n \oplus K_n)$$

- “一次一密”最早由Gilbert Vernam于1917年用于报文消息的自动加密和解密，并申请了专利。
- “一次一密”是定理2.4的特殊情况，满足完善保密性的充分条件。
- 一次一密无法抵抗已知明文分析，如果知道明文和对应的密文，就可以计算出密钥。
- 一次一密中要求n比特明文需要用n比特的密钥加密，这样为了发送密文，需要通信双方通过安全通道秘密协商好同样长度的密钥，不便于密钥管理，限制了商业应用。
- 流密码其实是模拟了“一次一密”，利用密钥流生成器由种子密钥生成密钥流，密钥流模拟了“一次一密”中只使用一次的密钥。

- 上一节讨论了密钥只用于一次加密时的完善保密性。
- 本节讨论密钥加密多个消息时，假设密码分析者有足够多的时间，进行一次成功的唯密文分析需要多长的密文。
- 信息熵是分析以上问题的工具，由Shannon在1948年提出。
  - 熵是信息或不确定性的数学度量；
  - 熵是随机变量**X**的概率分布的一个函数。
  - 熵的定义应该符合人们对信息的直觉。

熵

假设随机变量**X**在有限集合X上取值，则随机变量**X**的熵定义为

$$H(\mathbf{X}) = -\sum_{x \in \mathbf{X}} Pr[x] lbPr[x]$$

其中函数$lb(x) = \log_2(x)$。

熵和编码的关系：

- 随机变量**X**的熵表示了对随机变量中的每个可能事件进行二进制编码的期望长度的下限，并且随着$|X| \to \infty$，对随机变量**X**的二进制编码的期望长度趋向于它的熵。
- 使用Huffman编码时，随机变量**X**的二进制编码期望长度最小。令$l(f)$表示X的Huffman编码的期望长度，则有

$$H(X) \leq l(f) \leq H(x) + 1$$

例2.5：假设$X = \{a, b, c, d, e\}$有如下概率分布：$Pr[a] = 0.05$，$Pr[b] = 0.1$，$Pr[c] = 0.12$，$Pr[d] = 0.13$，$Pr[e] = 0.6$。Huffman编码结果如下：

a	000	b	001	c	010
d	011	e	1		

编码的期望长度为：

$$l(f) = 0.05 \times 3 + 0.10 \times 3 + 0.12 \times 3 + 0.13 \times 3 + 0.60 \times 1 = 1.8$$

熵为：

$$H(\mathbf{X}) = 1.7402$$

熵的性质

1. $H(\mathbf{X}) \geq 0$。
2. $H(\mathbf{X})$衡量的是随机变量$\mathbf{X}$的不确定性，不确定性越大，那么X中一个事件发生获得的信息越大。
3. $H(\mathbf{X}) = 0 \Longleftrightarrow$对某个$x_0 \in X$，$Pr[x_0] = 1$，对所有$x \neq x_0, Pr[x] = 0$。直观意义：如果$x_0$的发生是完全确定的，那么信息为0，或者不确定性为0。
4. 如果$|X| = n$，$H(\mathbf{X}) \leq lbn$，等式成立当且仅当$Pr[x] = \frac{1}{n}$，$x \in X$。直观意义：当每个事件发生的概率均等时，不确定性达到最大，那么事件发生时获得的信息是最大的。

熵的性质（续）

- $H(X,Y) \le H(X) + H(Y)$，等式成立当且仅当**X**和**Y**统计独立。直观意义：如果
  - 随机变量**X**和**Y**分别表示小王微积分成绩和代数成绩，
  - $H(\mathbf{X})$和$H(\mathbf{Y})$分别表示小王微积分成绩和代数成绩的不确定性，
  - $H(X,Y)$表示小王的微积分成绩和代数成绩的联合不确定性，

  因为小王的微积分和代数成绩很可能有关系（例如，如果微积分成绩好，那么代数成绩也好），因此同时两门成绩的联合不确定性不比它们的不确定之和大。
  如果**X**和**Y**分别表示小王的微积分成绩和小李的代数成绩，而且他们互不相识，各自的成绩相互独立，那么他们的成绩联合不确定性是各自的不确定性之和。

条件熵

假设**X**和**Y**是两个随机变量。对于**Y**的任何固定值y，得到一个**X**上的（条件）熵概率分布，记相应的随机变量为$\mathbf{X}|y$。显然

$$H(\mathbf{X}|y) = -\sum_{x} Pr[x|y]lbPr[x|y]$$

定义条件熵$H(\mathbf{X}|\mathbf{Y})$为熵$H(\mathbf{X}|y)$取遍所有的y的加权平均值（数学期望）。计算公式为

$$H(\mathbf{X}|\mathbf{Y}) = -\sum_{y}\sum_{x} Pr[y]Pr[x|y]lbPr[x|y]$$

条件熵度量了**Y**揭示的**X**的平均信息量。

条件熵的性质：

- $H(\mathbf{X},\mathbf{Y}) \leq H(\mathbf{Y}) + H(\mathbf{X}|\mathbf{Y})$。
- $H(\mathbf{X}|\mathbf{Y}) \leq H(\mathbf{X})$，等式成立当且仅当$\mathbf{X}$和$\mathbf{Y}$统计独立。

定理2.10

设$(\mathcal{P},\mathcal{C},\mathcal{K},\mathcal{E},\mathcal{D})$是一个密码体制，那么：

$$H(\mathbf{K}|\mathbf{C}) = H(\mathbf{K}) + H(\mathbf{P}) - H(\mathbf{C})$$

说明：

- $H(\mathbf{K}|\mathbf{C})$称为密钥含糊度，度量了给定密文情况下密钥的不确定性。
- 直观意义：截获密文后，密钥的的未知信息量等于明文与密钥总的未知信息量减去从已知的密文中获得的信息量。
- 该定理用于后面估计伪密钥的期望数。

伪密钥：攻击者Oscar从获取的密文中确定出密钥的可能值范围，但是仅有一个值是正确密钥，那些无法排除但不正确的可能密钥称为伪密钥。

例：Oscar获得移位密码加密的密文串WANJW，而且知道明文是某一自然语言，分析知道只有2个密钥的解密结果为有意义明文串，分别为

密钥	解密明文
5	river
22	arena

那么这两个可能密钥中只有一个是正确的，一个是伪密钥。

如果明文是有意义的，对给定密文，伪密钥数量的期望值是多少？
直观感觉：明文的不确定性（熵）越小，那么对固定长度的密文，伪密钥的数量应该越少，反之越大。
因此从自然语言L的熵H_L入手。H_L直观感觉应该是有意义明文串中每个字母的平均信息的度量：

- 如果L是随机分布独立统计的字母串，那么它的熵达到最大，为$lb(26) = 4.7$。
- 如果$\mathbf{P}$表示单个字母的随机变量，那么$H_L \approx H(\mathbf{P})$，对英文$H(\mathbf{P}) \approx 4.19$。
- 如果$\mathbf{P^2}$表示双个字母的随机变量，那么得到更精确的估计$H_L \approx \frac{H(\mathbf{P^2})}{2}$。
- 如果$\mathbf{P^n}$表示n个字母的随机变量，那么得到更精确的估计$H_L \approx \frac{H(\mathbf{P^n})}{n}$，并且$n$越大越精确。

从上面的讨论引发以下定义：

定义2.7

假设L是自然语言，语言L的（单字母）熵定义为

$$H_L = \lim_{n\to\infty} \frac{H(\mathbf{P^n})}{n}$$

语言L的冗余度定义为

$$\begin{aligned} R_L &= 1 - \frac{\text{语言L的熵}}{\text{随机语言的熵}} \\ &= 1 - \frac{H(H_L)}{lb|\mathcal{P}|} \\ &\simeq 1 - \frac{\text{语言L压缩后单个字母的期望编码长度}}{\text{语言L压缩前单个字母的编码长度}} \end{aligned}$$

说明：H_L度量了语言L的每个字母的平均熵，一个随机语言具有熵$lb|\mathcal{P}|$。因此R_L度量了“多余字母”的比例，即冗余度。

对英语，$H(P) = 4.19$，$H(P^2)/2 = 3.9 \ldots H(P^8)/8 = 2.3$，经验证实$1.0 \leq H_L \leq 1.5$。
如果英语的熵为1.25：

- 冗余度为3/4
- 英语的平均信息内容大概是每个字母1.25比特
- 数据压缩的意义：无损压缩编码可以把英文原文压缩到原来的1/4（1-冗余度），每个字母的平均长度为1.25比特。

以下证明略。如果$|\mathcal{P}| = |\mathcal{C}|$，密文串的长度为$n$时，伪密钥的期望数记为$\bar{s}_n$，当$n$充分大时，

$$lb(\bar{s}_n + 1) \geq H(\mathcal{K}) - nR_L lb|\mathcal{P}|$$

或写成

$$\bar{s}_n \geq \frac{|\mathcal{K}|}{|\mathcal{P}|^{nR_L}} - 1$$

- 可见，可通过提高密钥的熵来增加唯密文攻击所需平均密文量的长度，当密钥等概率选取时密钥熵达到最大值$lb|\mathcal{K}|$，这时得到以下定理2.11。

定理2.11

假设$(\mathcal{P},\mathcal{C},\mathcal{K},\mathcal{E},\mathcal{D})$是一个密码体制，$|\mathcal{C}|=|\mathcal{P}|$ 并且密钥是等概率选取的(大部分密码体制满足此条件)。设R_L表示明文的自然语言的冗余度，那么给定一个充分长（长为n）的密文串，伪密钥的期望数$\overline{s_n}$满足

$$\overline{s_n} \geq \frac{|\mathcal{K}|}{|\mathcal{P}|^{nR_L}} - 1$$

- 如果$R_L > 0$，$\frac{|\mathcal{K}|}{|\mathcal{P}|^{nR_L}}$以指数速度趋近于0
- 如果n很小，$H(P^n)/n$可能对H_L的估计不够好，将影响到对R_L的估计精确性，那么上面对$\overline{s_n}$的上界估计就可能不精确了。

定义2.8

一个密码体制的唯一解距离定义为使得伪密钥的期望数等于0的n的值，记为n_0，即在给定的足够的计算时间下分析者能唯一计算出密钥所需密文的平均值。

- 在定理2.11中，令$\overline{s_n} = 0$，解出n可得出唯一解距离的近似估计：

$$n_0 = \frac{lb|\mathcal{K}|}{R_L lb|\mathcal{P}|}$$

- 例：对代换密码，$|\mathcal{P}| = 26, |\mathcal{K}| = 26!$，英语的冗余值$R_L \approx 0.75$，那么代入上面估计公式得到唯一解距离为：

$$n_0 = 88.4/(0.75 \times 4.7) \approx 25$$

那么给定的密文串的长度至少为25时，通常解密才是唯一的。

- 如果语言是无意义，即$H_L = lb|\mathcal{P}|$，那么语言的冗余度$R_L = 0$，唯一解距离估计值

$$n_0 = \frac{lb|\mathcal{K}|}{R_L lb|\mathcal{P}|} = \infty$$

这说明当$|\mathcal{P}| = |\mathcal{C}|$且密钥是等概率选取时，无论敌手拥有多少计算资源，都无法从密文中唯一确定出密钥来。

- n_0和R_L成反比，这提示我们，在加密前压缩数据，以减少明文冗余度，可增加唯密文攻击的困难性。

- 乘积密码由Shannon在1949年提出，给出现代密码的迭代设计思想。
- 乘积密码的思想是由不安全的简单的密码体制通过迭代的方法构造出安全复杂的密码体制。
- 注意，由简单密码构造的乘积密码并不一定比简单密码安全。

为简单起见，假定$\mathcal{C} = \mathcal{P}$，这样的密码体制称为内嵌式密码体制。设有两个密码体制$S_1 = (\mathcal{P}, \mathcal{P}, \mathcal{K}_1, \mathcal{E}_1, \mathcal{D}_1)$，$S_2 = (\mathcal{P}, \mathcal{P}, \mathcal{K}_2, \mathcal{E}_2, \mathcal{D}_2)$，定义$S_1$和$S_2$的乘积密码体制$S_1 \times S_2$为：

$$(\mathcal{P}, \mathcal{P}, \mathcal{K}_1 \times \mathcal{K}_2, \mathcal{E}, \mathcal{D})$$

加密和解密规则定义为：对任意的$K \in (K_1, K_2)$，

$$e_{(K_1,K_2)}(x) = e_{K_2}(e_{K_1}(x))$$

$$d_{(K_1,K_2)}(y) = d_{K_1}(d_{K_2}(y))$$

而且密钥空间$\mathcal{K}$的概率分布如下：

$$Pr[(K_1, K_2)] = Pr[K_1] \times Pr[K_2]$$

即，分别根据定义在$\mathcal{K}_1$和$\mathcal{K}_2$上的概率分布，独立的选择K_1和K_2。

例：定义乘法密码的$\mathcal{P}=\mathcal{C}=\mathbb{Z}_{26}$，并且

$$\mathcal{K}=\{a\in\mathbb{Z}_{26}:\gcd(a,26)=1\}$$

对于$a\in K$，加密和解密定义如下：

$$e_a(x)=ax \bmod 26$$

$$d_a(y)=a^{-1}y \bmod 26$$

如果M是乘法密码（密钥等概率选取），S是移位密码（密钥等概率选取，加密函数为$e_K=x+K \bmod 26$），那么：

●$M\times S$是仿射密码。证明：其密钥(a,K)的加密形式为：

$$e_{(a,K)}(x)=(ax+K) \bmod 26$$

所以$M\times S$的密钥(a,K)相当于仿射密码的密钥(a,K)，这是$1-1$对应关系，而且对应的仿射密码的概率为$1/12\times 1/26=1/312$，证毕！

●$S\times M$是仿射密码。证明：$S\times M$中密钥(K,a)的加密形式为：

$$e_{(K,a)}(x)=a(x+K) \bmod 26=ax+ak \bmod 26$$

这样$S\times M$的密钥(K,a)等同于仿射密码的密钥(a,aK)，因为$\gcd(a,26)=1$，这是$1-1$对应关系，而且对应的仿射密码的概率为$1/12\times 1/26=1/312$，证毕！

- 对内嵌密码体制S_1, S_2, S_3，其乘积运算是可结合的（因合成函数具有结合性），即：

$$(S_1 \times S_2) \times S_3 = S_1 \times (S_2 \times S_3)$$

- 如果$S_1 \times S_2 = S_2 \times S_1$则称$S_1$和$S_2$可交换。如：乘法密码和移位密码可交换。
- $S \times S$记为S^2，S的n重乘积记为S^n。
- 如果$S^2 = S$则称密码体制S是幂等的。若S是幂等的，S^2不比S安全，反之，要通过多次迭代(即自己的多重乘积)提高安全性，密码体制必须不是幂等的
- 如果S_1和S_2都是幂等的且可交换，则可证$S_1 \times S_2$幂等。因此：$S_1 \times S_2$不幂等，就必须S_1, S_2不可交换。

总结

下面总结Shannon理论对密码设计的指导思想：

- 完善保密性($Pr(x|y) = Pr(y)$)是唯密文分析条件下的无条件安全，但因为完善保密的必要条件是$|\mathcal{K}| > |\mathcal{P}|$，这意味着密钥至少和明文一样长，这说明了完善保密的密码体制是不实用的。此外，完善保密在已知明文分析下可能不安全，如一次一密密码体制在已知明文分析下敌手可分析出密钥。
- 唯一解距离的估计值$n_0 = \frac{lb|\mathcal{K}|}{R_L lb|\mathcal{P}|}$和语言的冗余度$R_L$成反比，应先压缩后加密。
- 密钥等概率选取时，密钥的熵达到最大，此时唯密文分析唯一确定出密钥需要的密文量最大。
- 乘积密码给出了密码体制的迭代设计的方法，如果密码体制是幂等的，那么多重迭代无法提高安全性，用不幂等的密码体制多重迭代可能提高安全性。