目录

第一章　绪论

1.1　什么是密码学

如果我们要求一个从未接触过密码学的人处理一段文字，把这段文字尽可能地加密，让别人无法破解。那么，大多数人在深思熟虑之后，总能提出一些加密算法。比如说，著名的凯撒密码：把一段由英文字母组成的语句，每个字母都在字母表中往后移 3 个位置。“veni vidi vici” 也就变成了 “yhql ylgl ylfl”. 当问起这种密码体制里最重要的是什么，大部分人都会说是加密算法。如果把加密算法告诉了别人，那这种密码就相当于被破解了。

如果进而问起一个密码体制的组成，大部分人的回答，就是加密算法。也许有些自诩比普通人聪明一点的人，还会加上一个解密算法，也就是，将处理过后的密码变为正常文字的算法。如果用 m 代表要被加密的文字，c 代表被加密出来的密码，E() 代表加密算法，D() 代表解密算法，那么大多数人理解的密码学，本质就是以下这两个式子:

$$c = \mathrm{E}\left(m\right)$$
$$m = \mathrm{D}\left(c\right)$$

细想起来，这似乎不无道理。但是，拿凯撒密码为例，在其加密算法中，还有一个关键的量：3. 试想，如果通信双方 Alice 和 Bob, Alice 在场的所有人她用的是凯撒密码的加密方式加密她的话，又偷偷告诉 Bob 她使用的凯撒密码里，是将每个字母在字母表的位置上向后移动 4 个位置。那么，即使在场有人能偷听到 Alice 给 Bob 的密码，也无法破解 Alice 想说的是什么，只有掌握了规则“向后移动 4 个位置”的 Bob, 才能正确地破解密码。

如果还是按照之前的说法，一个密码体制包括加密算法和解密算法，那么向后移动 3 个位置的凯撒密码和向后移动 4 个位置的凯撒密码，就成了两个密码体制。但是，这两种加密方式是极其类似的，差别也就只在于一个向后移动 3 个位置，一个向后移动 4 个位置。我们对于这些密码的研究，也许也就十分类似。因此，把这两种加密方式归类为同一种密码体制，似乎是更好的选择。因此，密钥就应运而生了。所谓密钥，我们可以粗略地理解成加密算法、解密算法中的参数，也就是我们之前说的 3、4. 通过一个密码体制通信的双方，需要首先在保密信道中确定密钥。而一个密码体制，也就可以由加密算法、解密算法和密钥构成。因此，如果以 k 代表密钥，那么之前的式子就变成了

$$c = \mathrm{E}_k\left(m\right)$$
$$m = \mathrm{D}_k\left(c\right)$$

这也就是现在通用的密码学。

1.2 密码体制的基本要素

根据之前的讨论，我们就可以得出一个密码体制的基本要素：

- 明文空间 $\mathcal{M}$

  所有可以被加密算法加密的元素组成的集合，加密算法的定义域。明文空间的元素叫做明文 $m \in \mathcal{M}$.

  例如，在凯撒密码中，明文空间就为所有由英文字母组成的字符串。

- 密文空间 $\mathcal{C}$

  所有可以由加密算法输出的元素组成的集合，加密算法的值域。密文空间的元素叫做密文 $c \in \mathcal{C}$.

  我们需要注意到的是，这里的值域，可以理解成二元函数 $\mathrm{E}(k, m)$ 的值域。比如说，对于加密算法

  $$\mathrm{E}_k(m) = m^2 + k^2$$

  其密文空间为 $[0, +\infty)$ 而非 $[k^2, +\infty)$.

- 密钥空间 $\mathcal{K}$

  所有密钥组成的集合。密钥空间的元素叫做密钥 $k \in \mathcal{K}$.

  这里值得指出，在非对称加密算法中，密钥空间分为加密密钥空间和解密密钥空间。也就是说，在加密算法中使用的密钥，并不一定就是在解密算法中使用的密钥。

  此外，对于对称加密算法，也就是只用一个密钥的加密体制，密钥也并不一定是一个数。比如说，加密算法

  $$\mathrm{E}_{a,b}(m) = am + b$$

  我们仍认为其使用单一密钥 (a, b).

  此外，可不可能不存在密钥呢？确实有这样的密码体制，但这样却也十分不安全。比如说，加密算法

  $$\mathrm{E}(m) = m$$

  就是一个无密钥的加密算法。

- 加密算法 $\mathrm{E}_k(m)$

  根据密钥生成的特定算法，将明文转化为密文。

- 解密算法 $\mathrm{D}_k(c)$

  根据密钥生成的特定算法，将密文转化为明文。

  对于对称加密算法，也就是只使用一个密钥的加密体制，解密算法与加密算法满足

  $$\mathrm{D}_k(\mathrm{E}_k(m)) = m$$

在我们讨论密码体制的一些性质时，密钥生成算法有时也是必要的。什么是密钥生成算法呢？回忆之前 Alice 和 Bob 的例子，凭什么 Alice 选择的密钥是 4 而不是 25 呢？这就涉及到了密钥生成算法。在这个例子中，密钥生成算法就是 Alice 自己想到哪个密钥就输出哪个密钥。但是，从严格意义上来讲，密钥生成算法是一种概率算法。所谓概率算法，就是在算法的

步骤中涉及到了某些概率。比如说，在某个密钥生成算法中，在 $(0,1)$ 中等概率随机生成一个数 t, 而生成的密钥 k 满足

$$k=\begin{cases}1 & t\in(0.5,1)\\ 0 & t=0.5\\ -1 & t\in(0,0.5)\end{cases}$$

这就是一个典型的概率算法。其特点就是在两次运行中输出的结果不一定相同。

因此，我们称一个加密方案包含三个要素：加密算法 E, 解密算法 D, 密钥生成算法 G. 根据定义，我们可以说，一个密码体制由一个加密方案 $(\mathrm{E},\mathrm{D},\mathrm{G})$ 及一个明文空间 $\mathcal{M}$ 完全定义。

因此，Alice 和 Bob 的一次加密通信的过程包括：

1. Alice 根据密钥生成算法 G 生成密钥 $k\in\mathcal{K}$.
2. Alice 通过安全信道将 k 告诉 Bob.
3. Alice 将想要传达的明文 $m\in\mathcal{M}$ 根据加密算法加密成密文 $c=\mathrm{E}_k(m)$ 告诉 Bob.
4. Bob 根据之前 Alice 告诉自己的 k、密文 c 及解密算法得出明文 $m=\mathrm{D}_k(c)$

那么，在一个密码体制中，哪个最重要呢? 是不是之前我们说的加密算法呢? 这里，就不得不提 Kerckhoffs 原则。用现代的语言来说，Kerckhoffs 原则阐述的是：

提倡安全性不能建立在对算法的保密上。

也就是说，我们如果要证明一个加密体制的安全性，不能指望算法的保密性。我们应默认加解密算法可以被所有人知道（事实上也确实如此）。也就是说，真正值得保密的，是密钥。如果潜在的敌手获得密钥，那么根据公开的解密算法，那么他就可以从窃得的密文中获得明文。

1.3 加密系统的安全性

为了从数学上定义加密系统的安全性，我们必须引入一些和概率有关的定义。