为了生成 RSA 的公钥和私钥，Bob 执行如下步骤：

1）选择两个大素数 p 和 q。那么 p 和 q 应该多大呢？该值越大，破解 RSA 越困难，而执行加密和解密所用的时间也越长。RSA 实验室推荐，公司使用时，p 和 q 的乘积为 1024 比特的数量级。对于选择大素数的方法的讨论，参见［Caldwell 2012］。

2）计算 $n=pq$ 和 $z=(p-1)(q-1)$。

3）选择小于 n 的一个数 e，且使 e 和 z 没有（非 1 的）公因数。（这时称 e 与 z 互素。）使用字母 e 表示是因为这个值将被用于加密。

4）求一个数 d，使得 $ed-1$ 可以被 z 整除（就是说，没有余数）。使用字母 d 表示是因为这个值将用于解密。换句话说，给定 e，我们选择 d，使得

$$ed \bmod z = 1$$

5）Bob 使外界可用的公钥 K_B^+ 是一对数（n，e）；其私钥 K_B^- 是一对数（n，d）。

Alice 执行的加密和 Bob 进行的解密过程如下：

- 假设 Alice 要给 Bob 发送一个由整数 m 表示的比特组合，且 $m<n$。为了进行编码，Alice 执行指数运算 m^e，然后计算 m^e 被 n 除的整数余数。换言之，Alice 的明文报文 m 的加密的值 c 就是：

$$c = m^e \bmod n$$

  对应于这个密文 c 的比特模式发送给 Bob。

- 为了对收到的密文报文 c 解密，Bob 计算：

$$m = c^d \bmod n$$

  这要求使用他的私钥（n，d）。

举一个简单的 RSA 例子，假设 Bob 选择 $p=5$ 和 $q=7$。（坦率地讲，这样小的值无法保证安全。）则 $n=35$ 和 $z=24$。因为 5 和 24 没有公因数，所以 Bob 选择 $e=5$；最后，因为 $5\times29-1$（即 $ed-1$）可以被 24 整除，所以 Bob 选择 $d=29$。Bob 公开了 $n=35$ 和 $e=5$ 这两个值，并秘密保存了 $d=29$。观察公开的这两个值，假定 Alice 要发送字母“l”、“o”、“v”和“e”给 Bob。用 1~26 之间的每个数表示一个字母，其中 1 表示“a”，…，26 表示“z”，Alice 和 Bob 分别执行如表 8-2 和表 8-3 所示的加密和解密运算。注意到在这个例子中，我们认为每四个字母作为一个不同报文。一个更为真实的例子是把这四个字母转换成它们的 8 比特 ASCII 表示形式，然后加密对应得到的 32 比特的比特模式的整数。（这样一个真实的例子产生了一些长得难以在教科书中打印出来的数！）

假定在表 8-2 和表 8-3 中的简单示例已经产生了某些极大的数，并且假定我们前面看到 p 和 q 每个都是数百比特长的数，这些都是实际使用 RSA 时必须要牢记的。如何选择大素数？如何选择 e 和 d？以及如何对大数进行指数运算？对这些重要问题的详细讨论超出了本书的范围，详情请参见［Kaufman 1995］以及其中的参考文献。

表 8-2 Alice 的 RSA 加密，$e=5$，$n=35$

明文字母	m：数字表示	me	密文 $c=me \bmod n$
l	12	248832	17
o	15	759375	15
v	22	5153632	22
e	5	3125	10