明文报文“bob，i love you. alice”变成“nkn，s gktc wky. mgsbc”。因此，与用凯撒密码情况一样，这看起来像乱码。单码代替密码的性能看来要比凯撒密码的好得多，可能的字母配对为26!（为10^{26}数量级），而不是25种可能的配对。尝试所有的10^{26}种可能配对的蛮力法，其要求的工作量太大，不是一种破解加密算法和解密报文的可行方式。但是，通过对明文语言进行统计分析，例如，在典型的英语文本中，由于已知字母“e”和字母“t”出现的频率最高（这些字母出现的频率分别为13%和9%），还可知常见的二三个字母的组合通常一起出现（例如，“in”、“it”、“the”、“ion”、“ing”等等），这就使得破解该密文变得相对容易。如果入侵者具有某些该报文的可能内容的知识，则破解该密码就会更为容易。例如，如果入侵者Trudy是Bob的妻子，怀疑Bob和Alice有暧昧关系，则她可能猜想“bob”和“alice”这些名字可能会出现在密文中。如果Trudy确信这两个名字出现在密文中，并有了上述报文的密文副本，她则能够立即决定这26个字母配对中的7个，比蛮力法少检查10^9种可能性。如果Trudy的确怀疑Bob有不正当的男女关系，她可能也非常期待从该报文中找到某些其他选择的词汇。

当考虑Trudy破解Bob和Alice之间加密方案的难易程度时，可以根据入侵者所拥有的信息区分三种不同的情况。

- 唯密文攻击。有些情况下，入侵者只能得到截取的密文，也不了解明文报文的内容。我们已经看到，统计分析有助于对加密方案的**唯密文攻击**（ciphertext-only attack）。
- 已知明文攻击。前面已经看到，如果Trudy以某种方式确信在密文报文中会出现“bob”和“alice”，她就可以确定字母a、l、i、c、e、b和o的（明文，密文）匹配关系。Trudy也可能会幸运地记录到传输的所有密文，然后在一张纸上找到Bob写下的已解密的明文。当入侵者知道（明文，密文）的一些匹配时，我们将其称之为对加密方案的**已知明文攻击**（known-plaintext attack）。
- 选择明文攻击。在**选择明文攻击**（chosen-plaintext attack）中，入侵者能够选择某一明文报文并得到该明文报文对应的密文形式。对于我们前面所说的简单加密算法来说，如果Trudy能让Alice发送报文“The quick brown fox jumps over the lazy dog,”，则Trudy就能够完全破解Alice和Bob所使用的加密方案。但是随后我们将看到，对于更为复杂的加密技术来说，使用选择明文攻击不一定意味着能够攻破该加密机制。

500年前，发明了**多码代替密码**（polyalphabetic encryption），这种技术是对单码代替密码的改进。多码代替密码的基本思想是使用多个单码代替密码，一个单码代替密码用于加密某明文报文中一个特定位置的一个字母。因此，在某明文报文中不同位置出现的相同字母可能以不同的方式编码。图8-4中显示了多码代替密码机制的一个例子。它使用两个凯撒密码（其中$k=5$和$k=19$），如图中不同的行所示。我们可以选择使用这两个凯撒密码C_1和C_2，加密时采用以C_1，C_2，C_2，C_1，C_2的次序循环的模式即明文的第一个字母用C_1加密，第二和第三个字母用C_2编码，第四个字母使用C_1，第五个字母用C_2，然后循环重复该模式，即第六个字母用C_1加密，第七个字母用C_2加密，依此类推。这样一来，明文报文“bob，i love you.”加密后成为“ghu，n etox dhz.”。注意到明文报文中的第一个“b”用C_1加密为“g”，第二个“b”用C_2加密为“u”。在这个例子中，加密和解密“密钥”是两个凯撒密码密钥（$k=5$和$k=19$）和C_1，C_2，C_2，C_1，C_2的次序模式的知识。