§2.5 密码分析

密码分析学是在不知道密钥的情况下，恢复出明文的科学。成功的密码分析能恢复出消息的明文或密钥。密码分析也可以发现密码体制的弱点，最终得到上述结果（密钥通过非密码分析方式的丢失叫做泄露）。

常用的密码分析攻击有:

（1）唯密文攻击（Cipher Text-Only Attack）。

密码分析者有一些消息的密文，这些消息都用同一加密算法加密。密码分析者的任务是恢复尽可能多的明文，或者最好是能推算出加密消息的密钥来，以便可采用相同的密钥解出其他被加密的消息。

§2.5 密码分析

（2）已知明文攻击（Known-Plaintext Attack）。

密码分析者不仅可得到一些消息的密文，而且也知道这些消息的明文。分析者的任务就是用加密信息推出用来加密的密钥或推导出一个算法，此算法可以对用同一密钥加密的任何新的消息进行解密。

（3）选择明文攻击（Chosen-Plaintext Attack）。

密码分析者不仅可得到一些消息的密文和相应的明文，而且也可选择被加密的明文。这比已知明文攻击更有效。密码分析者能选择特定的明文块去加密，那些块可能产生更多关于密钥的信息，分析者的任务是推出用来加密消息的密钥或导出一个算法，此算法可对用同一密钥加密的任何新消息进行解密

§2.5 密码分析

（4）选择密文攻击（Chosen-Cipher Text Attack）

密码分析者能选择不同的被加密的密文，并可得到对应的解密的明文，例如密码分析者存取一个防窜改的自动解密盒，密码分析者的任务是推出密钥。

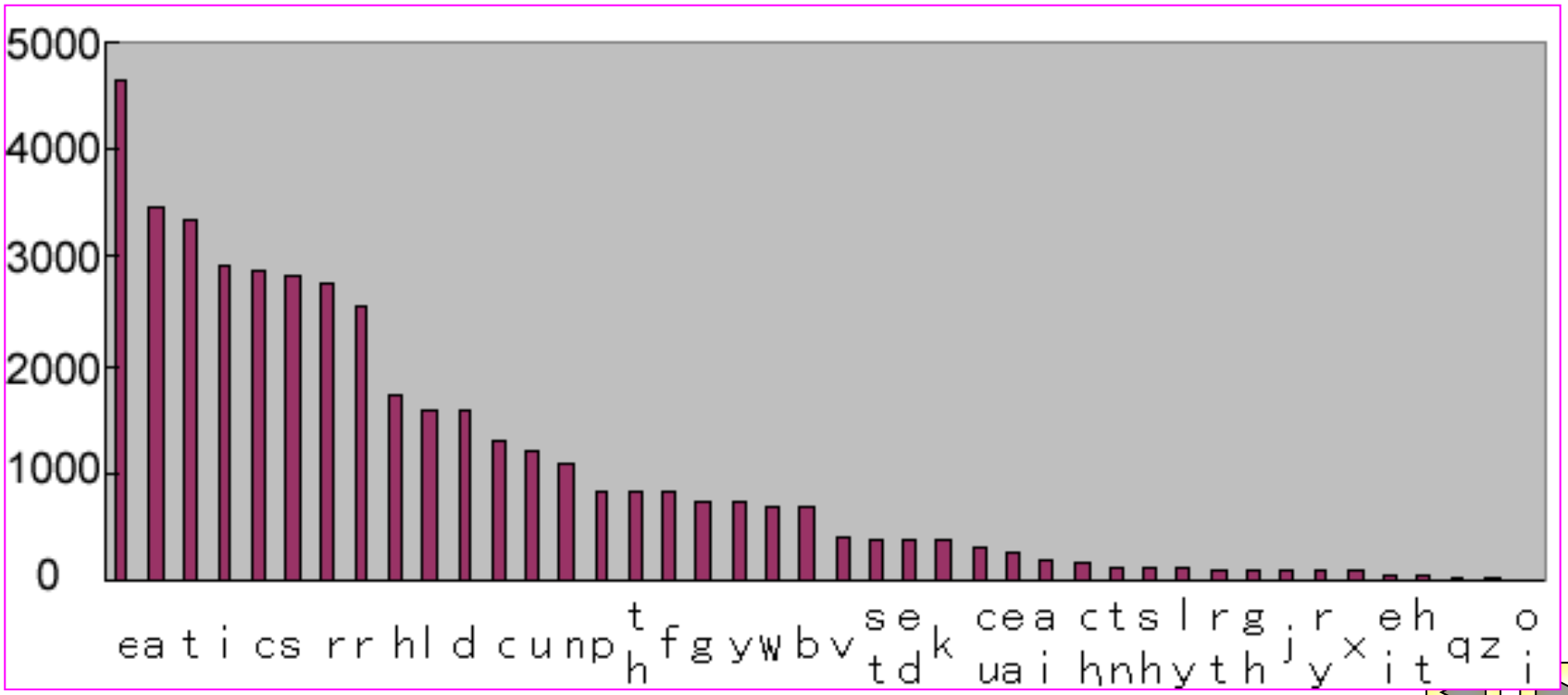
（5）软磨硬泡攻击（Rubber-Hose Cryptanalysis）

这种攻击是对密码分析者威胁、勒索，或者折磨某人，直到他给出密钥为止。行贿有时称为购买密钥攻击。这些是非常有效的攻击，并且经常是破译算法的最好途径。

§2.5 密码分析

单表密码分析：英语26个字母中，各字母出现的频率不同，经过大量统计，可以给出了各字母出现的频率值。

英文明文字母频度表



§2.5 密码分析

其次考虑字母连接频率（双字母组和三字母组出现频率）

再者考虑字母反复使用特征，英语单词以e、s、t、d结尾的超过一半；以t、a、s、w 为起始字母的约为一半。

某些常用用法也会提供有价值的线索，如信的开头写Dear；源程序的某一位置是版权声明；电子资金传送报头格式。

单表密码的弱点：明文和密文字母之间的一一代替关系。这使得明文中的一些固有特性和规律（比如语言的各种统计特性）必然反映到密文中去。

