§2.4 一次一密方案

一次一密方案是一种理想的加密方案。它使用的密钥是一个大的不重复的真随机密钥字母集，这个密钥字母集被写在几张纸上，并被粘成一个密码本。它最初的形式用于电传打字机。

发送者用密码本中的每一密钥字母准确地加密一个明文字符。加密是明文字符和一次密码本密钥字符的模26加法。

每个密钥仅对一个消息使用一次。发送者对所发送的消息加密，然后销毁密码本中用过的一页或磁带部分。接收者有一个同样的密码本，并依次使用密码本上的每个密钥去解密密文的每个字符。接收者在解密消息后销毁密码本中用过的一页或磁带部分。新的消息则用密码本中新的密钥加密。

§2.4 一次一密方案

例如，如果消息是：

ONE TIME PAD

而取自密码本的密钥序列是：

TBF RGFA RFM

那么密文就是：

IPK LPSF HGQ

因为

O＋T mode 26=I

N＋B mode 26=P

E＋F mode 26=K

……。