密码系统的组成
传统密码的密码体制
实用密码设备应必备的要素
ENIGMA 密码机原理
启示

密码学基本概念：起源于保密通信技术，是研究信息系统安全保密和认证的一门科学。
分为密码编码学和密码分析学（研究破解或攻击信息）
密码系统的组成：明文，密文，加密算法，解密算法，密钥（加密密钥，解密密钥）
传统密码体制是指采用手工或机械操作加解密的对称密码体制，安全性与加解密算法保密性密切相关
Kerckhoffs 认为安全性建立在密钥是保密的（而不是算法
传统密码体制：置换，代换（单表代换密码：凯撒，仿射；多表代换：维吉尼亚，Playfair，转轮
破解单表代换密码的方法：频率分析（明文字母出现频率与密文字母出现频率一致
多表代换密码加密：依照密钥轮流使用多个单表
Enigma 后人类迈入了机械化编码的时代（转轮密码机
Enigma：键盘，接线板（单表代换），扰频器（多表代换），反射器（加解密相同）
对付这样“暴力破译法”（即一个一个尝试所有可能性的方法），可以通过增加转子的数量来对付，因为只要每增加一个转子，就能使试验的数量乘上 26 倍

启示：加密系统的保密性只应建立在对密钥的保密上，不应该取决于加密算法的保密。这这是密码学中的金科玉律

实用密码设备应必备四要素：安全，性能，成本，易用