密码学：从艺术到科学

（一）Kerckhoffs原则：

原则内容：加密方案的安全性应仅依赖密钥保密，而非算法本身保密，即“算法可公开，密钥必私密”。

- **三大论证依据**
- - 密钥短于算法，更易保密，尤其在大规模应用中算法难以长期保密。
  - 密钥更新成本远低于算法替换，生成新密钥更便捷。
  - 公开算法可接受公众审查，提升安全性，避免“隐蔽式安全”的风险。

二、现代密码学的三大核心原则：严谨性的基石

（一）原则1：形式化定义——安全目标的精确刻画 - **定义的必要性**：无明确安全定义，无法判断方案是否达标（如“不可恢复密钥”非充分条件，“不可恢复明文”需细化）。 - **安全定义的构成** - **安全保证**：如加密方案应确保密文不泄露明文任何信息（而非仅“不可恢复全部明文”）。 - **威胁模型**：按攻击者能力分等级（唯密文攻击、已知明文攻击、选择明文攻击、选择密文攻击），不同场景需匹配相应模型。

（二）原则2：精确假设——安全证明的前提 - **假设的重要性**：现代密码学多依赖未被证明的计算复杂度假设（如(P≠NP)），需明确陈述。 - **假设的作用** - 可验证性：精确假设便于研究与验证，增强可信度。 - 可比较性：不同方案基于的假设可对比（如选择基于更弱或更成熟假设的方案）。 - 模块化：若底层假设被攻破，可替换组件而无需重设计方案。

（三）原则3：安全证明——对抗攻击的理论保障 - **证明的意义**：相对于定义与假设，提供“攻击者无法成功”的严格证明，避免依赖直觉（历史案例表明直觉在密码学中常出错）。 - **证明的局限性**：需匹配真实场景（如定义是否覆盖实际威胁，假设是否成立），但为攻防提供了理论框架。

（三）实践启示

-- **足够密钥空间原则**：安全加密方案的密钥空间必须足够大，使穷举攻击不可行。（古典密码简单代换密码:Caesar密码和移位密码（Shift Cipher））

--密钥空间大被误认为安全（只是基本条件），有可能败于统计分析。（古典密码单表代换密码，多表代换密码）

- 设计密码方案时，需先明确安全目标与威胁模型，再基于成熟假设构建并证明安全性(现代密码学与古典密码学的不同)。 - 避免“自创算法”，优先使用经过公开审查的标准方案（如AES），降低安全风险。