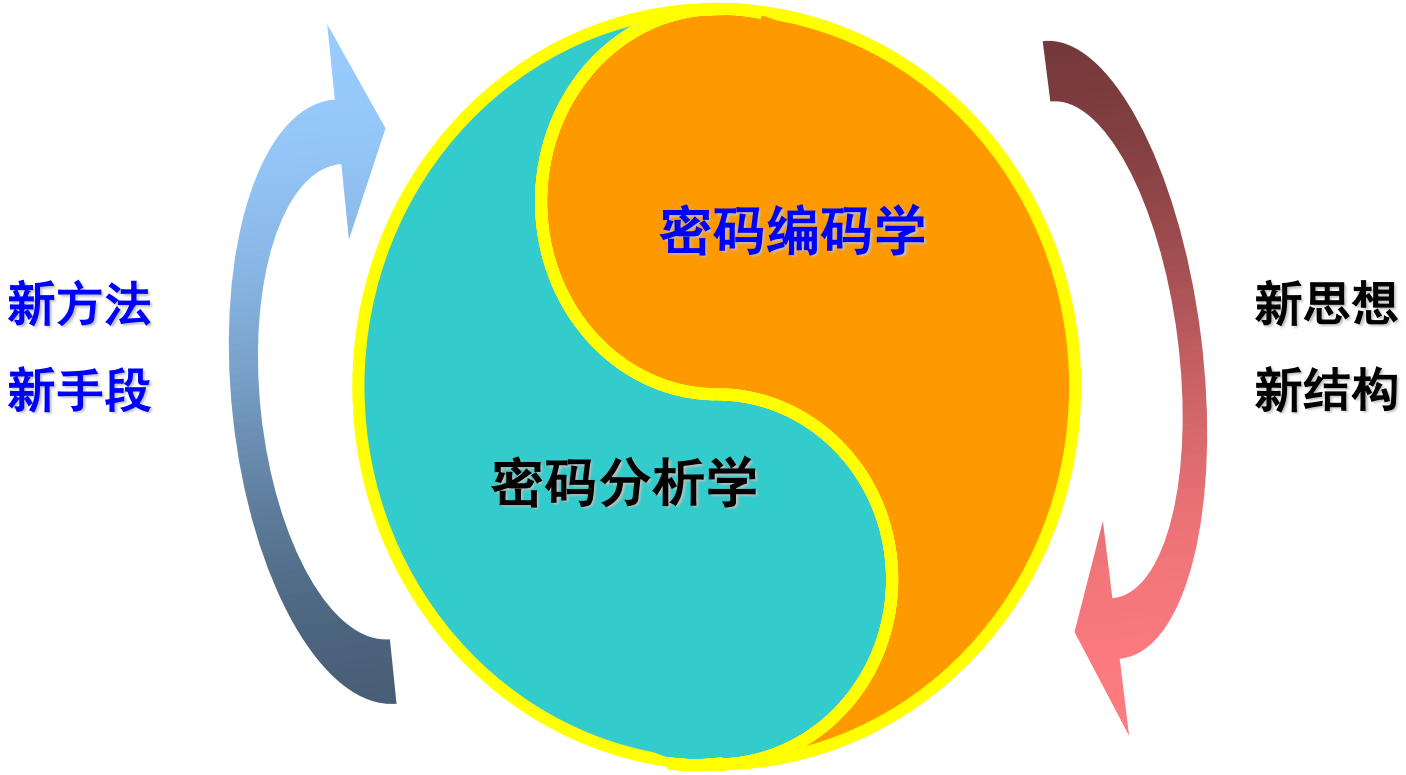
现代密码学

第五讲 密码分析学

信息与软件工程学院

密码学学科分支

- 两个分支形成既对立又统一的矛盾体



第五讲 密码分析学

- 安全的定义
- 密码分析方法的分类
- 无条件安全和计算上安全

安全的概念

“如果把一封信锁在保险柜中，把保险柜藏起来，然后告诉你去看这封信，这并不是安全，而是隐藏；

相反，如果把一封信锁在保险柜中，然后把保险柜及其设计规范和许多同样的保险柜给你，以便你和世界上最好的开保险柜的专家能够研究锁的装置，而你还是无法打开保险柜去读这封信，这才是安全…”

-Bruce Schneier

密码分析学的前提

- Kerckhoffs假设：假定密码分析者和敌手知道所使用的密码系统。即密码体制的安全性仅依赖于对密钥的保密，而不应依赖于算法的保密
  - 假设敌手知道：
  - （1）所使用的加密算法
  - （2）知道明文的概率分布规律；
  - （3）知道密钥的概率分布规律；
  - （4）知道所有可能的破译方法
  - （5）敌手能够拿到加密装置，可以对其进行能量消耗分析等等

一切秘密皆蕴含在密钥中！

密码分析学的目标

- 恢复合法密文相应的明文
- 恢复密钥

第五讲 密码分析学

- 安全的定义
- 密码分析方法的分类
- 无条件安全和计算上安全

密码体制的攻击方法

密码分析者攻击密码体制的方法：

（1）穷举攻击：通过试遍所有的密钥来进行破译。

对抗：可增大密钥的数量。

（2）统计分析攻击：通过分析密文和明文的统计规律来破译。

对抗：设法使明文和密文的统计规律不一样。

（3）解密变换攻击：针对加密变换的数学基础，通过数学求解设法找到解密变换。

对抗：选用具有坚实的数学基础和足够复杂的加密算法。

密码体制的攻击（密码破译）

攻击强度

- 唯密文攻击（Ciphertext Olny Attack）
- 已知明文攻击（Known Plaintext Attack）
- 选择明文攻击（Chosen Plaintext Attack）
- 选择密文攻击（Chosen Ciphertext Attack）

这里一切的目的在于破译出密钥或者密文！

惟密文攻击

- 密码分析者仅知道一些密文。
- 最困难，一般是穷搜索，对截获密文用所有可能密钥去试
- 惟密文攻击敌手知道的信息量最少，最易抵抗
- 只要有足够的计算时间和存储容量，原则上可成功，但在实际上一种能保证安全要求的实用密码算法，都会设计得这一方法在实际上不可行
- 一般的敌手需要对密文进行统计测试分析，为此需要知道被加密的明文类型，英文文本，图象等。

已知明文攻击

- 密码分析者知道一些明文和相应的密文。
- 在很多情况下，敌手可能有更多的信息，也许能够截获一个或多个明文及其对应的密文，或消息中将出现某种明文格式，这时的攻击称为已知明文攻击，敌手也许能从已知的明文被变换成密文的方式得到密钥

选择明文攻击

- 密码分析者可以选择一些明文，并得到相应的密文。
- 如果攻击者能在加密系统中插入自己选择的明文消息，则通过该明文消息对应的密文有可能确定出密钥的结构
- 明文可以是精心选择的

选择密文攻击

- 密码分析者可以选择一些密文，并得到相应的明文。
- 攻击者利用解密算法，对自己所选的密文解密出相应的明文，有可能确定出密钥信息
- 选择的密文可以与要破解的密文相关

第五讲 密码分析学

- 安全的定义
- 密码分析方法的分类
- 无条件安全和计算上安全

无条件安全与计算上安全

- 无条件安全的(不可破译的)：
  - 无论截获多少密文，都没有足够信息来唯一确定明文，则该密码是无条件安全的，即对算法的破译不比猜测有优势
- 计算上安全的：
  - 使用有效资源对一个密码系统进行分析而未能破译，则该密码是强的或计算上安全的

密码算法要满足的准则

密码算法只要满足以下两条准则之一就行：

（1） 破译密文的代价超过被加密信息的价值。

（2 ）破译密文所花的时间超过信息的有用期。

满足以上两个准则的密码算法在实际中是可用的。

感 谢 聆 听!

xynie@uestc.edu.cn