第四讲　常规加密

--- 分组密码

上海交通大学安全学院
郑燕飞

AES

* DES已走到了它生命的尽头，其56比特密钥实在太小，三重DES只是在一定程度上解决了密钥长度问题。另外，DES的设计主要针对硬件实现，而今在许多领域，需要用软件方法来实现它，在这种情况下，DES效率相对较低。1997年4月15日美国国家标准和技术研究所（NIST）发起征集AES（AES—Advanced Encryption Standard）算法的活动，并成立了AES工作组，目的是为了确定一个非保密的、公开披露的、全球免费使用的加密算法，用于保护下一世纪政府的敏感信息。AES的基本要求是比三重DES快而且至少和三重DES一样安全，分组长度128比特密钥长度为128/192/256比特。

AES候选算法（续1）

* 要求

--- 比三重DES快，至少还要一样的安全，

--- 应当具有128比特分组长度和256比特分组密钥长度（不过必须支持128和192比特的密钥）

--- 还应该具有较大的灵活性。

AES候选算法（续2）

* 评选过程中采用的方法

1.用量化的或定性的尺度作为选择的标准；
2.选择一种以上的算法；
3.选择一个备用算法；
4.考虑公众的建议以改进算法。

AES候选算法（续3）

1998年8月20日，NIST在第一阶段讨论（AES1）中宣布了由12个国家提出的15个候选算法

1999年3月开始的第二阶段讨论（AES2），

1999年8月NIST选出5个算法候选：

MARS、RC6、Rijndael、Serpent和Twofish。

AES候选算法-过程（续4）

在宣布最后的5个候选算法后，NIST再次恳请公众参与对这些算法的评论。公众对这五种候选算法的评阅期于2000年5月15日结束。NIST发布的AES主页[2]提供了大量的关于算法描述、源程序、有关AES3的论文以及其他公众评论的信息。2000年4月开始进行第三阶段（AES3）的评选，AES3共收到37篇提交给NIST的论文，并采用了其中的24篇。在这一阶段的讨论中，这些算法得到了非常深入的分析。NIST的AES小组综合所有公众对候选算法的评价和分析作了一个非常彻底的评论。

AES候选算法-过程（续5）

经过长时间的评审和讨论之后，NIST在2000年5月宣布选择Rijndael作为AES的算法。该算法的开发者提出以下几种发音供选择"Reign Dah1"，"Rain doll"和 "Rhine Dah1"。

AES候选算法（续6）

* 结果

NIST最终选择了Rijndael作为AES的标准，因为全面地考虑，Rijndael汇聚了安全，性能好，效率高，易用和灵活等优点。Rijndael使用非线性结构的S-boxes，表现出足够的安全余地；Rijndael在无论有无反馈模式的计算环境下的硬，软件中都能显示出其非常好的性能；它的密钥安装的时间很好，也具有很高的灵活性；Rijndael的非常低的内存需求也使它很适合用于受限的环境；

AES候选算法-结果（续）

Rijndael的操作简单，并可抵御时间和能量攻击，此外，它还有许多未被特别强调的防御性能；Rijndael在分组长度和密钥长度的设计上也很灵活，算法可根据分组长度和密钥长度的不同组合提供不同的迭代次数，虽然这些特征还需更深入地研究，短期内不可能被利用，但最终，Rijndael内在的迭代结构会显示良好的潜能来防御入侵行为。

AES参数

	密钥长度(N_k字)	分组大小(N_b字)	迭代轮数(N_r)
AES-128	4	4	10
AES-192	6	4	12
AES-256	9	4	14

AES演示

AES演示

其他常规密码

- Blowfish
- RC5
- CAST-128
- RC2
- 这些都是比较先进的对称分组密码
  - 可变密钥长度
  - 混合操作使密码分析复杂化
  - 依赖于数据或密钥的循环移位
  - …

END