现代密码学

第二十七讲 AES算法简介

信息与软件工程学院

第二十七讲 AES算法简介

- AES提出的背景
- AES算法框架和参数说明

AES标准算法征集

- DES算法由于其密钥较短，难以抵抗现有的攻击，因此不再作为加密标准
- 1997年1月，美国NIST向全世界密码学界发出征集21世纪高级加密标准（AES——Advanced Encryption Standard）算法的公告，并成立了AES标准工作研究室，1997年4月15日的例会制定了对AES的评估标准。

AES算法征集的要求

（1）AES是公开的；

（2）AES为对称密钥分组密码体制；

（3）AES的密钥长度可变，可按需要增大；

（4）AES适于用软件和硬件实现；

（5）AES可以自由地使用，或按符合美国国家标准（ANST）策略的条件使用。

算法衡量条件

- 满足以上要求的AES算法，需按下述条件判断优劣
  - 安全性
  - 计算效率
  - 内存要求
  - 使用简便性
  - 灵活性

AES的评审

- 1998年4月15日全面征集AES算法的工作结束。1998年8月20日举行了首届AES讨论会，对涉及14个国家的密码学家所提出的候选AES算法进行了评估和测试，初选并公布了15个被选方案，供大家公开讨论。

  CAST-256，RC-6，CRYPTON-128，DEAL-128，

  FROG，DFC，LOKI-97，MAGENTA，

  MARS，HPC，RIJNDAEL，SAFER+，

  SERPENT，E-2，TWOFISH。

- 这些算法设计思想新颖，技术水平先进，算法的强度都超过3-DES，实现速度快于3-DES。

AES的评审（续）

- 1999年8月9日NIST宣布第二轮筛选出的5个候选算法为：

  MARS(C.Burwick等,IBM），

  RC6™（R. Rivest等,RSA Lab.),

  RIJNDEAL(J. Daemen,比利时),

  SERPENT(R. Anderson等，英国、以利时、挪威),

  TWOFISH(B. Schneier，美国)。

- 2000年10月2日，NIST宣布Rijndael作为新的AES

第二十七讲 AES算法简介

- AES提出的背景
- AES算法框架和参数说明

AES算法设计思想

- 设计简单
- 在多个平台上速度快，编码紧凑
- 抵抗所有已知的攻击
- Rijndael没有采用Feistel结构，轮函数由3个不同的可逆均匀变换构成的，称为3个层
  - 均匀变换是指状态的每个bit都用类似的方法处理

轮函数的3层

- 线性混合层
  - 确保多轮之上的高度扩散；
- 非线性层
  - 将具有最优的“最坏情况非线性特性”的S盒并行使用；
- 密钥加层
  - 单轮子密钥简单的异或到中间状态上，实现一次性掩盖。

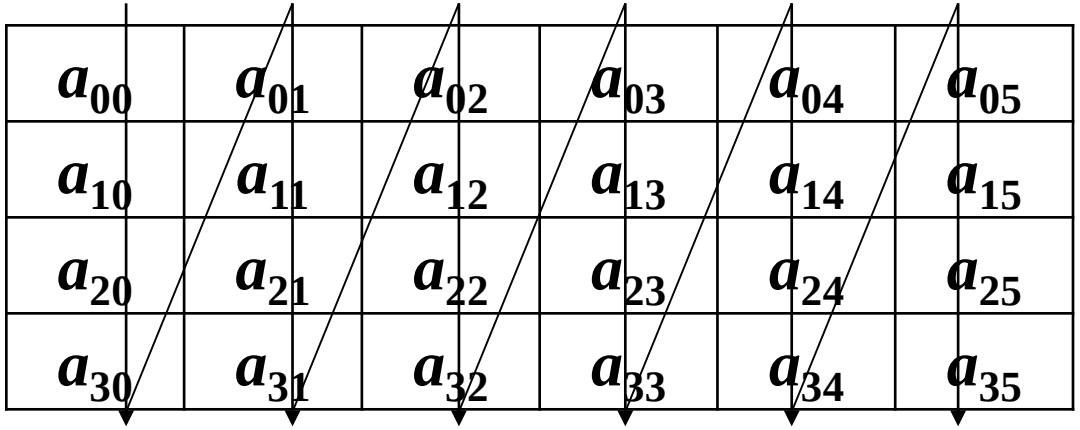
算法说明

- 明文分组可变，128、192、256比特
- 密钥长度可变，各自可独立指定为128、192、256比特。
- 状态
  - 算法中间的结果也需要分组，称之为状态，状态可以用以字节为元素的矩阵阵列表示，该阵列有4行，列数N_b为分组长度除32
- 种子密钥
  - 以字节为元素的矩阵阵列描述，阵列为4行，列数N_k为密钥长度除32

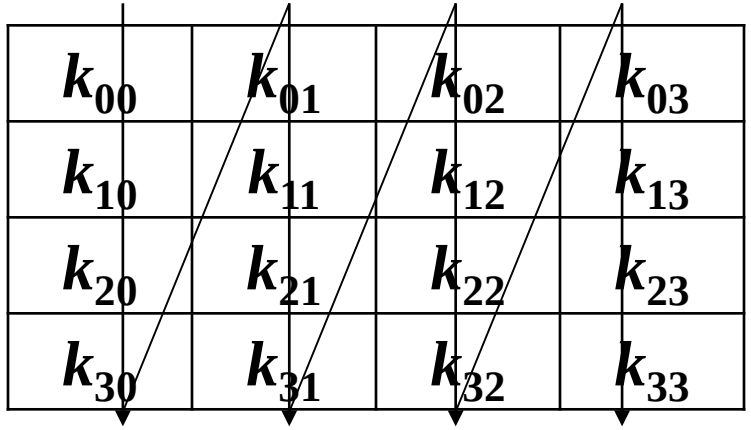
算法说明

- 算法的输入、输出和种子密钥可看成字节组成的一维数组。
- 下标范围
  - 输入输出：**0—$4N_b$-1**
  - 种子密钥：**0—$4N_k$-1**

N_b=6和N_k=4的状态密钥阵列



按此顺序放入和读出

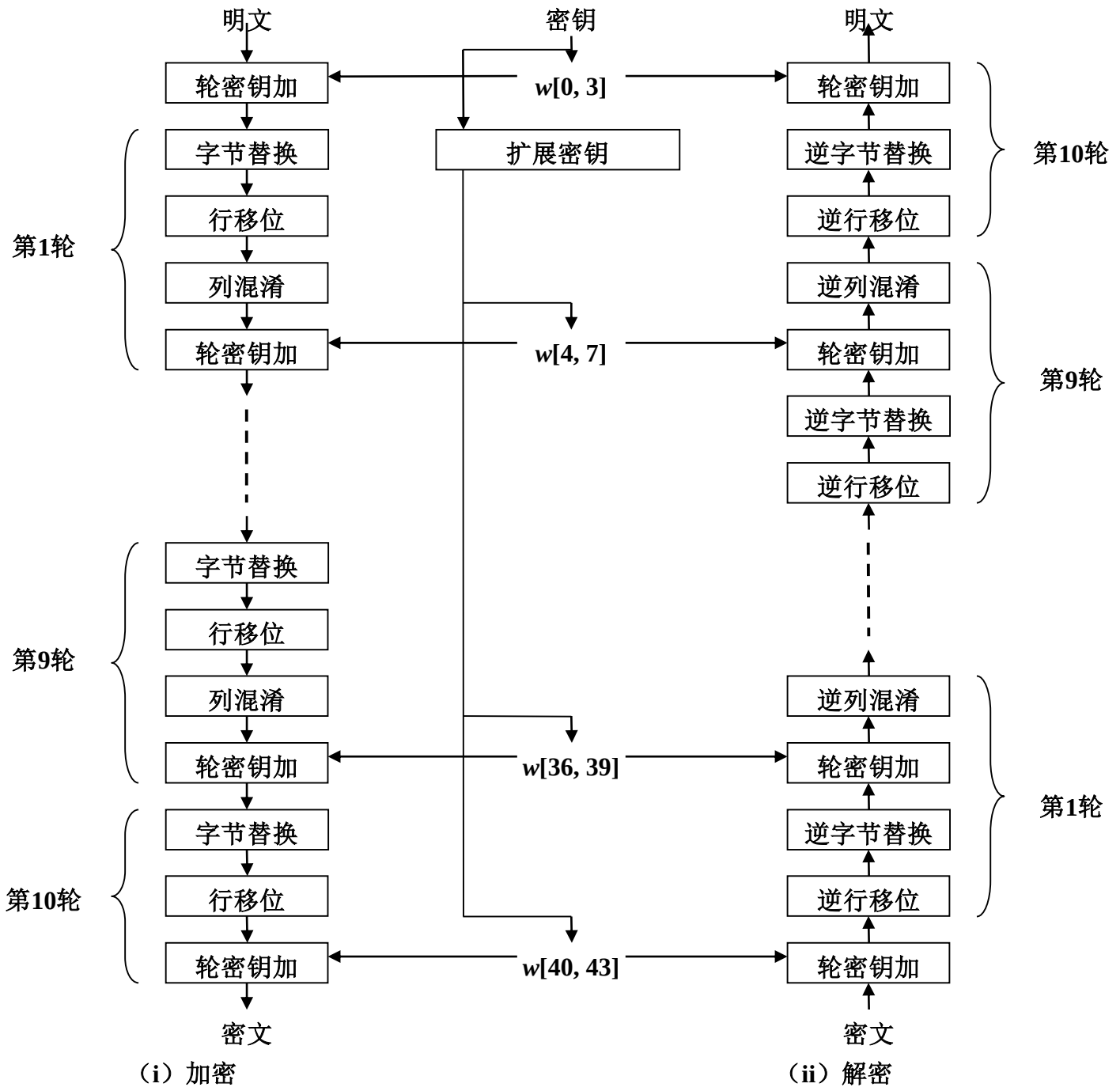


按此顺序放入

分组和阵列中元素对应关系

- 分组下标n
- 阵列位置(i,j)
  - i=n mod 4, j=[n/4];n=i+4j
- 轮数N_r与N_b和N_k对应关系

	N_b=4	N_b=6	N_b=8
N_k=4	10	12	14
N_k=6	12	12	14
N_k=8	14	14	14


明文
密钥
明文
轮密钥加
w[0, 3]
轮密钥加
字节替换
扩展密钥
逆字节替换
第10轮
行移位
逆行移位
第1轮
列混淆
逆列混淆
轮密钥加
w[4, 7]
轮密钥加
第9轮
逆字节替换
逆行移位
字节替换
逆列混淆
第9轮
行移位
列混淆
轮密钥加
w[36, 39]
轮密钥加
第1轮
字节替换
逆字节替换
第10轮
行移位
逆行移位
轮密钥加
w[40, 43]
轮密钥加
密文
密文
（i）加密
（ii）解密

感 谢 聆 听!

xynie@uestc.edu.cn