Symmetric-key algorithm

1简介

对称密钥加密（英语：Symmetric-key algorithm）又称为对称加密、私钥加密、共享密钥加密，这类算法在加密和解密时使用相同的密钥，常见的对称加密算法有[DES](https://zh.wikipedia.org/wiki/%E8%B3%87%E6%96%99%E5%8A%A0%E5%AF%86%E6%A8%99%E6%BA%96" \o "资料加密标准)、[3DES](https://zh.wikipedia.org/wiki/3DES" \o "3DES)、[AES](https://zh.wikipedia.org/wiki/%E9%AB%98%E7%BA%A7%E5%8A%A0%E5%AF%86%E6%A0%87%E5%87%86" \o "高级加密标准)

(1)在[密码学](https://zh.wikipedia.org/wiki/%E5%AF%86%E7%A0%81%E5%AD%A6" \o "密码学)中，分组加密（英语：Block cipher），又称分块加密或块密码，是一种[对称密钥算法](https://zh.wikipedia.org/wiki/%E5%AF%B9%E7%A7%B0%E5%AF%86%E9%92%A5%E7%AE%97%E6%B3%95" \o "对称密钥算法)。它将明文分成多个等长的模块（block），使用确定的算法和[对称密钥](https://zh.wikipedia.org/wiki/%E5%AF%B9%E7%A7%B0%E5%AF%86%E9%92%A5" \o "对称密钥)对每组分别加密解密。分组加密是极其重要的加密协议组成，其中典型的如[DES](https://zh.wikipedia.org/wiki/DES" \o "DES)和[AES](https://zh.wikipedia.org/wiki/%E9%AB%98%E7%BA%A7%E5%8A%A0%E5%AF%86%E6%A0%87%E5%87%86" \o "高级加密标准)作为美国政府核定的标准加密算法，应用领域从电子邮件加密到银行交易转帐，非常广泛。

DES

数据加密标准（英语：Data Encryption Standard，缩写为 DES）是一种[对称密钥加密](https://zh.wikipedia.org/wiki/%E5%B0%8D%E7%A8%B1%E5%AF%86%E9%91%B0%E5%8A%A0%E5%AF%86" \o "对称密钥加密)[块密码](https://zh.wikipedia.org/wiki/%E5%A1%8A%E5%AF%86%E7%A2%BC" \o "块密码)算法,DES现在已经不是一种安全的加密方法，主要因为它使用的56位密钥过短。

|  |  |
| --- | --- |
| [密钥](https://zh.wikipedia.org/wiki/%E5%AF%86%E9%92%A5" \o "密钥)长度 | 56位 |
| [块长度](https://zh.wikipedia.org/w/index.php?title=%E5%9D%97%E9%95%BF%E5%BA%A6&action=edit&redlink=1" \o "块长度（页面不存在）) | 64位 |

3DES

三重数据加密算法（英语：Triple Data Encryption Algorithm，缩写为TDEA，Triple DEA），或称3DES（Triple DES），是一种[对称密钥加密](https://zh.wikipedia.org/wiki/%E5%B0%8D%E7%A8%B1%E5%AF%86%E9%91%B0%E5%8A%A0%E5%AF%86" \o "对称密钥加密)[块密码](https://zh.wikipedia.org/wiki/%E5%A1%8A%E5%AF%86%E7%A2%BC" \o "块密码)，相当于是对每个数据块应用三次[数据加密标准](https://zh.wikipedia.org/wiki/%E8%B3%87%E6%96%99%E5%8A%A0%E5%AF%86%E6%A8%99%E6%BA%96" \o "数据加密标准)（DES）算法。由于计算机运算能力的增强，原版DES密码的[密钥长度](https://zh.wikipedia.org/wiki/%E5%AF%86%E9%92%A5%E9%95%BF%E5%BA%A6" \o "密钥长度)变得容易被[暴力破解](https://zh.wikipedia.org/wiki/%E6%9A%B4%E5%8A%9B%E7%A0%B4%E8%A7%A3" \o "暴力破解)；3DES即是设计用来提供一种相对简单的方法，即通过增加DES的密钥长度来避免类似的攻击，而不是设计一种全新的块密码算法。

|  |  |
| --- | --- |
| [密钥](https://zh.wikipedia.org/wiki/%E5%AF%86%E9%92%A5" \o "密钥)长度 | 168，112或56 位 |
| [块长度](https://zh.wikipedia.org/w/index.php?title=%E5%9D%97%E9%95%BF%E5%BA%A6&action=edit&redlink=1" \o "块长度（页面不存在）) | 64位 |

AES

高级加密标准（英语：Advanced Encryption Standard，[缩写](https://zh.wikipedia.org/wiki/%E7%B8%AE%E5%AF%AB" \o "缩写)：AES），在[密码学](https://zh.wikipedia.org/wiki/%E5%AF%86%E7%A0%81%E5%AD%A6" \o "密码学)中又称Rijndael加密法，是[美国联邦政府](https://zh.wikipedia.org/wiki/%E7%BE%8E%E5%9B%BD%E8%81%94%E9%82%A6%E6%94%BF%E5%BA%9C" \o "美国联邦政府)采用的一种[区块加密](https://zh.wikipedia.org/wiki/%E5%8D%80%E5%A1%8A%E5%8A%A0%E5%AF%86" \o "区块加密)标准。这个标准用来替代原先的[DES](https://zh.wikipedia.org/wiki/DES" \o "DES)，已经被多方分析且广为全世界所使用。2006年，高级加密标准已然成为[对称密钥加密](https://zh.wikipedia.org/wiki/%E5%AF%B9%E7%A7%B0%E5%AF%86%E9%92%A5%E5%8A%A0%E5%AF%86" \o "对称密钥加密)中最流行的[算法](https://zh.wikipedia.org/wiki/%E6%BC%94%E7%AE%97%E6%B3%95" \o "算法)之一。

|  |  |
| --- | --- |
| [密钥](https://zh.wikipedia.org/wiki/%E5%AF%86%E9%92%A5" \o "密钥)长度 | 128、192或者256比特 |
| [块长度](https://zh.wikipedia.org/w/index.php?title=%E5%9D%97%E9%95%BF%E5%BA%A6&action=edit&redlink=1" \o "块长度（页面不存在）) | 128位 |

(2)流加密（英语：Stream cipher），又译为串流加密、资料流加密，是一种[对称加密](https://zh.wikipedia.org/wiki/%E5%AF%B9%E7%A7%B0%E5%8A%A0%E5%AF%86" \o "对称加密)算法，加密和解密双方使用相同伪随机加密数据流（pseudo-random stream）作为[密钥](https://zh.wikipedia.org/wiki/%E5%AF%86%E9%92%A5" \o "密钥)，[明文](https://zh.wikipedia.org/wiki/%E6%98%8E%E6%96%87" \o "明文)数据每次与密钥数据流顺次对应加密，得到[密文](https://zh.wikipedia.org/wiki/%E5%AF%86%E6%96%87" \o "密文)数据流。实践中数据通常是一个[位](https://zh.wikipedia.org/wiki/%E4%BD%8D" \o "位)（bit）并用[异或](https://zh.wikipedia.org/wiki/%E5%BC%82%E6%88%96" \o "异或)（xor）操作加密。

该算法解决了对称加密[完善保密性](https://zh.wikipedia.org/wiki/%E5%AE%8C%E5%96%84%E4%BF%9D%E5%AF%86%E6%80%A7" \o "完善保密性)（perfect secrecy）的实际操作困难。由于完善保密性要求密钥长度不短于明文长度，故而实际操作存在困难，改由较短数据流通过特定算法得到密钥流。

RC4

RC4（来自Rivest Cipher 4的缩写）是一种[流加密](https://zh.wikipedia.org/wiki/%E6%B5%81%E5%8A%A0%E5%AF%86" \o "流加密)算法，[密钥](https://zh.wikipedia.org/wiki/%E5%AF%86%E9%92%A5" \o "密钥)长度可变。它加解密使用相同的密钥，因此也属于[对称加密算法](https://zh.wikipedia.org/wiki/%E5%AF%B9%E7%A7%B0%E5%8A%A0%E5%AF%86" \o "对称加密)。RC4是[有线等效加密](https://zh.wikipedia.org/wiki/%E6%9C%89%E7%B7%9A%E7%AD%89%E6%95%88%E5%8A%A0%E5%AF%86" \o "有线等效加密)（WEP）中采用的加密算法，也曾经是[TLS](https://zh.wikipedia.org/wiki/%E4%BC%A0%E8%BE%93%E5%B1%82%E5%AE%89%E5%85%A8%E5%8D%8F%E8%AE%AE" \o "传输层安全协议)可采用的算法之一。RC4由[伪随机数](https://zh.wikipedia.org/wiki/%E4%BC%AA%E9%9A%8F%E6%9C%BA%E6%95%B0" \o "伪随机数)生成器和[异或](https://zh.wikipedia.org/wiki/%E5%BC%82%E6%88%96" \o "异或)运算组成。RC4的密钥长度可变，范围是[1,255]。RC4一个字节一个字节地加解密。