**凯撒加密法**

一种简单移位加密法，明文中的每个字母被其后的n个字母替换

**加密法**

基于使用密钥的某种算法，将消息打乱

**密文**

一个被打乱的消息

**编码法**

通过用字、短语或数字替换明文来打乱信息的一种方法

**密码分析法**

破解编码和加密的一门艺术与科学

**解密**

还原被打乱信息的过程

**加密**

打乱消息的过程

**单码加密法**

具有固定替换模式的加密法，即明文的每个字母就由密文的一个字母替代

**明文**

可读的消息

**多码加密法**

一种加密法，其替换模式是，可以用多个字母来替代同一个明文字母

**夹带法**

通过隐藏消息的存在来隐藏信息的方法

**替换加密法**

用一个字符替换另一个字符的方法

**换位加密法**

重新排列明文中字母的位置的加密法

**连字**

文字中一对相邻近的字母

**频率分析法**

将明文字母的出现频率与密文字母的频率相比较的过程

**GCD**

最大公约数，即给定两个数，GCD就是能整除这两个数的最大数字

**单码加密法**

明文的每个字母只能被密文的一个字母替代的加密法

**自动密钥法**

一种通过把明文或密文作为部分密钥，从而扩展密钥长度的方法

**de Visaris方法**

一种已知明文攻击法，通过扫描圆柱面的正确排列顺序来破解圆柱面加密法

**一致性索引**

由William Friedman设计，用来测试多码加密密文

**同音异义加密法**

一种将每个明文字母用多个密文符号来替换的加密法

**Kasiski法**

这种方法通过查看重复密文部分，来发现多码密钥的长度

**多码加密法**

一种将每个明文字母用多个密文字母来替换的加密法

**回转轮加密法**

一种多码加密法，它使用多个回转轮，每个回转轮实现单码加密。这些回转轮可以组合在一起，在每个字母加密后产生一种新的替换模式

**Hill 加密法**

一种基于矩阵相乘的多图加密法

**Playfair加密法**

一种使用一个关键词方格来加密字符的加密法

**多图加密法**

一种一次将两个或多个字符加密的加密法

**列加密法**

一种换位加密法，其中，明文按行写入到一个矩阵中，然后以一定的顺序读取列以生成密文

**双重列加密法**

一种换位加密法，他首先应用列换位加密法生成一个中间密文，然后用另一个换位加密法将中间密文加密成最终密文

**单图换位**

一种重新排列字母的换位加密法

**多图换位**

一种重新排列单词或字母的换位加密法

**换位加密法**

一种重新排列密文字母顺序的换位加密法

**A5**

一种基于LFSR的流加密法，用于移动电话的安全保护

**单元自动操作**

对数组中的单个单元进行操作，其中，各单元的值取决于其相邻单元和指定的规则

**CRC**

循环冗余校验，一种用于确保消息完整性的方法

**LFSR**

线性反馈移位寄存器，一种数组电路，他保存有n位。他将各位置上的位向右移动，并用选定的一些位来填充最左位

**MUX**

复用器，一种数组电路，他有2的n次方个输入和一个输出，根据一定的原则选取其中一个输入作为输出

**一次性纸板**

一种流加密法，其中的密钥位模式永不重复，这是唯一一种已证实是不可破解的加密法

**RC4**

一种广泛使用的流加密法，他可以很容易地在软件中实现

**同步加密法**

密钥流与信息流无关的加密法

**自同步流加密法**

密钥流依赖于前面n个密文字符的加密法

**WEP**

无线等效保密，该协议使用RC4加密法来保护无线传输

**AES**

高密加密标准，在经历长时间的检查和评估后，选择了Rijndael

**ASIC**

应用特定集成电路

**CBC**

加密块链，像自动密钥加密法一样使用块加密法

**CTR**

计数器模式，使用块加密法来生成类似于流加密法的密钥

**DES**

数据加密标准

**差分密码分析法**

一种用于破解块加秘法的已知明文攻击法

**ECB**

电子编码薄模式，用相同的密钥加密每个块

**FPGA**

现场可编程门阵列

**ICM**

整数计数器模式，像流加密法一样使用块加密法

**IV**

初始向量，使用一些块加密法中，用来增加安全性

**线性密码分析法**

破解块加密法的已知明文攻击法

**中间点攻击法**

中间点攻击法

**S盒**

替换盒，作为一种非线性转换用在块加密法中

**EIGamal加密法**

一种公钥加密法，其安全性是基于求解离散对数问题的困难度的

**椭圆曲线**

曲线上的整数坐标点加法运算可以用来创建一种加密系统

**基因算法**

一种随机查找算法，基于生物学的自然选择特征

**背包加密法**

一种基于求解子集和问题的困难度的加密法

**公钥加密系统**

一种具有两个密钥的加密系统，公钥用于将明文加密，私钥用于解密

**RSA**

一种广泛使用的公钥加密系统，其安全性是基于将大整数因子分解的困难度

**重复平方法**

一种用来减少RSA所需的乘法次数的方法

**旁道密码分析法**

通过监视加密法实现的特征，来破解加密法的一种方法

**生日问题**

找到房间中有两个人生日相同的机会为50%所需的人数

**盲签名**

在不查看文档的情况下签署文档

**证书**

将公钥值绑定到所有人身上的过程

**DSS**

1994年采用的数字签名标准

**MD5**

Ron Rivest 开发的一种散列算法

**填充**

散列前在消息末尾增加额外比特位的过程

**公钥基础设施**

一种用于建立公钥系统中用户之间信任关系的可靠和安全的系统

**SHA**

NIST开发的安全散列算法

**SSL**

安全套接层，用于互联网提供应用的安全性

**验证**

验证证书依然有效的过程