（1）AES算法原理  
 AES加密算法是密码学中的高级加密标准。AES为分组加密法，把明文分成每组长度相等的一组一组；每次加密一组数据，直至整个明文被加密完毕。在AES标准规范中，分组长度只能是128位。AES是按照字节进行加密的，也就是说每个分组为16个字节（每个字节8位）。密钥的长度可以使用128位、192位或256位，但这会导致密钥长度不同，推荐加密的轮数也不同。

因为DES算法的不安全性，DES加密算法可以被破解。而3DES加密算法虽然还没有被破解，但是因其加解密效率低，所以基本上大家现在都会偏向使用AES算法。可以说，AES算法的提出就是为了替代DES算法。以下是AES算法的基本原理：

1.密钥选择： AES支持128位、192位和256位三种密钥长度。选择适当的密钥长度对于安全性至关重要。

2.分组和轮数： AES将数据分为固定大小的块，每个块的大小为128位。算法的轮数取决于密钥长度，分别为10轮（128位密钥）、12轮（192位密钥）和14轮（256位密钥）。

3.子密钥生成： 从输入密钥派生一系列子密钥。这些子密钥用于每一轮的轮密钥加操作。

4.初始轮密钥加： 将明文与初始轮密钥进行按位异或运算。

5.轮运算： AES算法包括几个轮运算，其中包括SubBytes（字节替代）、ShiftRows（行移位）、MixColumns（列混淆）和AddRoundKey（轮密钥加）。

SubBytes： 使用S盒替代每个字节，提高非线性性。

ShiftRows： 对每行进行循环左移，使数据更加分散。

MixColumns： 利用固定矩阵进行列混淆，增强混淆性。

AddRoundKey： 将轮密钥按位异或到数据中。

6.最终轮运算： 最后一轮没有MixColumns操作。

7.密文生成： 完成所有轮运算后，得到加密后的密文。