什么是AES？

AES是一种密码强度很高的对称密码算法，但是如果需要商用的话要向NIST支付授权费用。

怎么算AES？

跟DES一样，AES也是由多轮运算组成的。其中每一轮都包括：SubBytes，ShiftRows，MixColumns和AddRoundKey这四个步骤。

SubBytes

在AES的规范中，Rijindael的分组长度固定为128bits，密钥长度有128，192和256bits三种。

128bits就是16字节。一个字节可以表示0-255的任意值。而SubBytes就是根据其值在一个拥有256个值的替换表中查找出对应的值进行处理。

为了便于理解，大家可以将其看成是简单的替换。



ShiftRows

SubBytes 之后，我们就可以进行shiftRows的操作了。

由于我们的源字节是16bytes，可以将其看成4\*4 的一个矩阵。

ShiftRows就是将一行4字节按照一定的规则向左平移，现在有4行，每一行的平移字节数是不同的。

MixColumns

ShiftRows之后就是MixColumns，MixColumns是在4字节的列上面进行一定的运算，将其变为另外的4字节列。

AddRoundKey

最后将生产的字节和密钥进行XOR运算，最后生产结果。通常需要重复进行10-14轮运算。

Rijndael的特点

输入的所有bits都会在一轮里面被加密。同DES相比，AES的加密效率更加高效。

Rijndael 加密过程为：SubBytes->shiftRows->MixColumns->AddRoundKey , 解密的时候需要按照相反的流程来进行：AddRoundKey->MixColumns->shiftRows->SubBytes。 注意，除了AddRoundKey是XOR运算不需要逆运算之外，其他的步骤都需要进行逆运算。