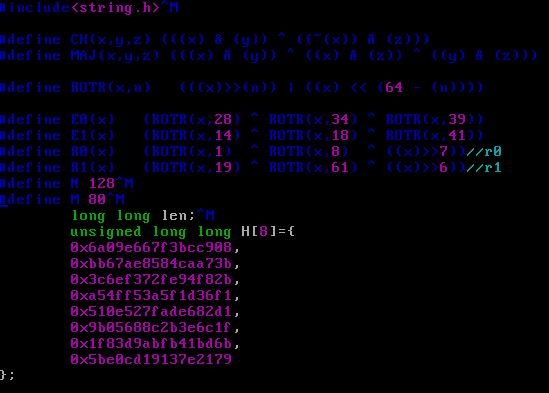
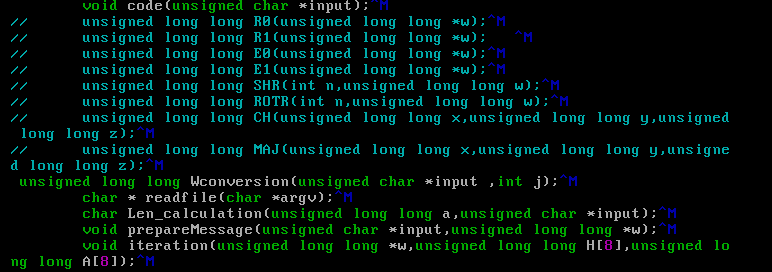
sha512算法的实现

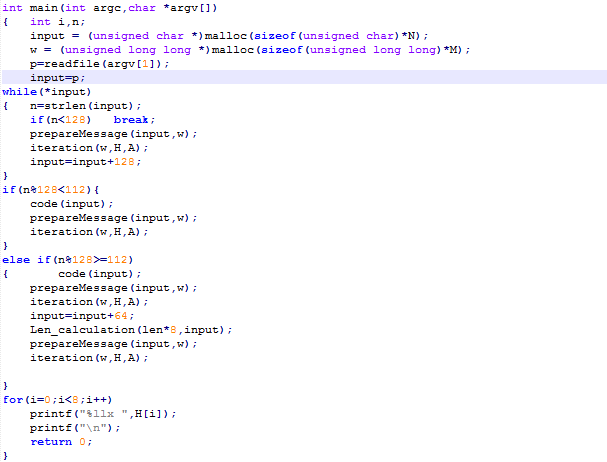
首先和前两种算法一样，sha512程序在声明头文件后建加入相关全局变量的定义如H1-H8、还有迭代准备值W， K的值，以及对程序中运用到的一些小算法（如ROTR、SHR、CH、MAJ）进行宏定义。



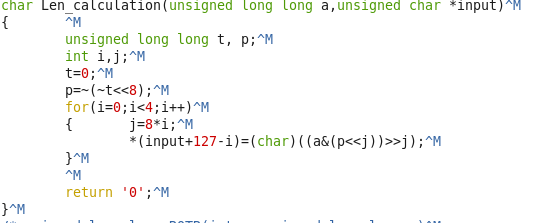
但是sha512和sha1、sha256不同的是sha512使用的是long long类型定义相关变量和函数的。



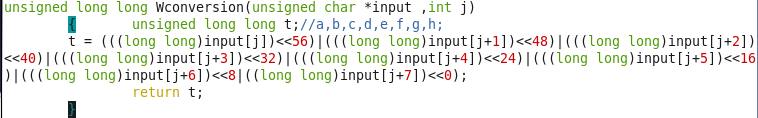
sha512的主函数与之前的sha256大体都是相同的。



但是在计算文件字符长度的时候，因为input要计算的是1024位的，所以函数Len\_calculation(…)需要修改。



且程序从迭代准备值生成的函数中将8位的\*input转换为64位的W准备值的函数也需要重新编写：



Input转换W



迭代准备值的生成：

最后定义的是iteration（…）函数，这个和sha256中的iteration（…）函数运算方法一样所以不需要修改。



程序进行运算，如果文件读取的长度，即\*p的长度大于128（1024位）时，程序一直循环，进行prepareMessage（…）和iteration（…）的运算。（其中将p指针的 地址赋值给input指针，input自增128个字符进行循环）一直计算到\*input的长度小于128是跳出循环，进行下一个判断。

当input的长度小于112时，进行补0 运算，然后将长度以16进制赋值到input的后128位中。进行最后一次迭代运算，输出值。

当input的长度大于112时，进行补0运算，然后迭代运算一次，再开辟128个长度（1024位）在新的input的后128位中赋值长度的16进制数，进行最后一次迭代运算，输出值。

然后使用sha512sum命令验证：

