This program is intended to Design an encryption system using only the MD5 function.

This encryption system should have the following steps:

1. Define a key to be shared with the receiver;
2. Calculate the MD5 hash of the defined key
3. Split the hex representation of the plaintext in equal blocks of the size of the hex representation of the MD5 hash;
   * For the last block, let consider M= size of (MD5 hash), B= size of the last block
   * If B < M then add (M- (B mod M)) “0”s at the front of the last block to complete the size to M
4. XOR the first block of the plaintext with the MD5 Hash
5. For each block starting from the second till the last block, calculate the MD5 Hash of the previous calculated MD5 then use it to XOR with the current block
6. The cipher text is obtained by joining all together in the order they occur, the results of the XOR

The program name is “cipherhash” and it is written with c language under the eclipse IDE.

For this program to run, user must:

1. run **apt-get install libssl-dev** onKali linux to install the developer library of openssl.
2. Extract the zip file to the workspace and go to program folder
3. Compile the compile the program by running the following command line: gcc -Wall -o "cipherhash" cipherhash/Debug/src/cipherhash.o -lcrypto -lssl
4. Use ./cipherhash to execute the program.
5. Provide a filename when asked by the program: “plaintext.text” is a sample file available in the program folder. (the file provided by the user must be in the program folder)
6. Run gcc -Wall -o "cipherhash" cipherhash/Debug/src/cipherhash.o -lcrypto -lssl -g -fno-stack-protector to use gdb
7. add the following “-lcrypto –lssl” to the linker flags under Eclipse > Project > Properties > c/c++ builder > settings>Cross Gcc linker> Miscellaneous in oder To be able to edit the program .

A successful buffer overflow exploit should be to prevent the program to provide the appropriate cipher text