**Task 5: Programming the Crypto Library**

#include <stdio.h>

#include <string.h>

#include <stdlib.h>

#include <openssl/evp.h>

int main()

{

int i;

char words[16], t;

FILE \*key, \*outFile;

const char \*out = "Output.txt";

unsigned char outbuf[1024 + EVP\_MAX\_BLOCK\_LENGTH];

unsigned char iv[] = "aabbccddeeff00998877665544332211";

int outlen, tmplen;

int num;

EVP\_CIPHER\_CTX ctx;

EVP\_CIPHER\_CTX\_init(&ctx);

char inText[] = "This is a top secret.";

char cipherText[] = "00000007969f17b638d4e79bade7d0726a291f0000010d9a49d89ee30ce5283d28808090cf0df0000020";

key = fopen("dictionary.txt", "r");

if( remove("ciphertext.txt") == -1 ) {

perror("Error deleting file");

}

outFile = fopen("ciphertext.txt", "a+");

if( key < 0 || outFile < 0 )

{

perror ("Cannot open file");

exit(1);

}

char pbuffer[1024];

while ( fgets(words,16, key) )

{

i=strlen(words);

words[i-1]='\0';

//printf("%s",words);

i = 0;

EVP\_EncryptInit\_ex(&ctx, EVP\_aes\_128\_cbc(), NULL, words, iv);

if(!EVP\_EncryptUpdate(&ctx, outbuf, &outlen, inText, strlen(inText)))

{

EVP\_CIPHER\_CTX\_cleanup(&ctx);

return 0;

}

if(!EVP\_EncryptFinal\_ex(&ctx, outbuf + outlen, &tmplen))

{

EVP\_CIPHER\_CTX\_cleanup(&ctx);

return 0;

}

outlen += tmplen;

print\_hex(outbuf, outlen, outFile);

}

fclose(key);

fclose(outFile);

return 1;

}

int print\_hex(unsigned char \*buf, int len, FILE \*outFile)

{

int i,n;

char x='\n';

for ( i = 0; i < len; i++ )

{

fprintf(outFile,"%02x",buf[i]);

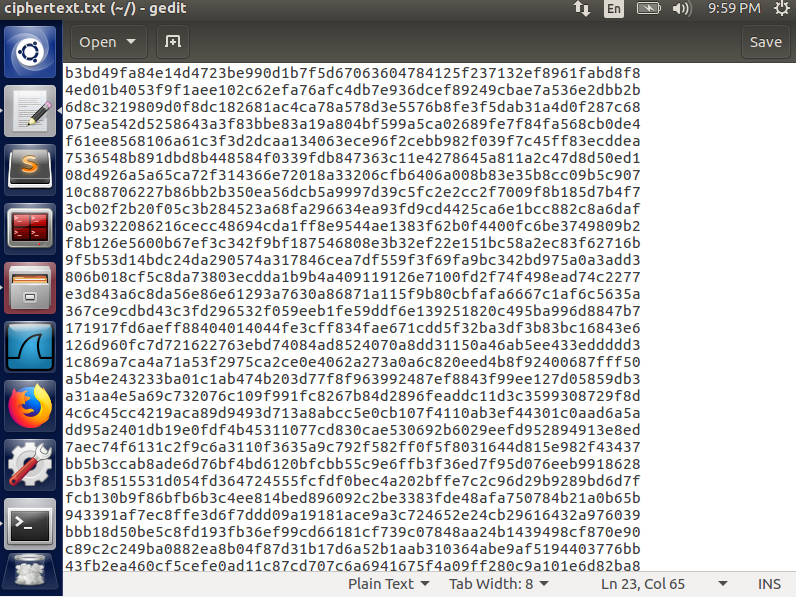
}

fprintf(outFile,"%c",x);

return (0);

}

**Output:**



I have written a C program that creates a file with all ciphers. Each time, I run the code, the cipher text is completely different. The given cipher text is encrypted purely with a word from the dictionary.txt file without any hashing.