|  |
| --- |
| 09/24/2019 |

|  |
| --- |
| CMPSC 443 Lab 1 |

# Task 1

I started by looking for the letter that appears the most, and saw that it is ‘n’ and assumed it can be replaced with e. After that I looked for the next letters that appear the highest bigram frequencies and it was ‘yt’ which I assumed it is ‘th’ and replaced that too.  
and I did saw a lot of “THE” in the text.  
after that I continued a bit with the letters and their frequencies and a bit with reading the text and guessing.



The decrypted text-

THE OSCARS TURN ON SUNDAY WHICH SEEMS ABOUT RIGHT AFTER THIS LONG STRANGE

AWARDS TRIP THE BAGGER FEELS LIKE A NONAGENARIAN TOO

THE AWARDS RACE WAS BOOKENDED BY THE DEMISE OF HARVEY WEINSTEIN AT ITS OUTSET

AND THE APPARENT IMPLOSION OF HIS FILM COMPANY AT THE END AND IT WAS SHAPED BY

THE EMERGENCE OF METOO TIMES UP BLACKGOWN POLITICS ARMCANDY ACTIVISM AND

A NATIONAL CONVERSATION AS BRIEF AND MAD AS A FEVER DREAM ABOUT WHETHER THERE

OUGHT TO BE A PRESIDENT WINFREY THE SEASON DIDNT JUST SEEM EXTRA LONG IT WAS

EXTRA LONG BECAUSE THE OSCARS WERE MOVED TO THE FIRST WEEKEND IN MARCH TO

AVOID CONFLICTING WITH THE CLOSING CEREMONY OF THE WINTER OLYMPICS THANKS

PYEONGCHANG

ONE BIG QUESTION SURROUNDING THIS YEARS ACADEMY AWARDS IS HOW OR IF THE

CEREMONY WILL ADDRESS METOO ESPECIALLY AFTER THE GOLDEN GLOBES WHICH BECAME

A JUBILANT COMINGOUT PARTY FOR TIMES UP THE MOVEMENT SPEARHEADED BY

POWERFUL HOLLYWOOD WOMEN WHO HELPED RAISE MILLIONS OF DOLLARS TO FIGHT SEXUAL

HARASSMENT AROUND THE COUNTRY

SIGNALING THEIR SUPPORT GOLDEN GLOBES ATTENDEES SWATHED THEMSELVES IN BLACK

SPORTED LAPEL PINS AND SOUNDED OFF ABOUT SEXIST POWER IMBALANCES FROM THE RED

CARPET AND THE STAGE ON THE AIR E WAS CALLED OUT ABOUT PAY INEQUITY AFTER

ITS FORMER ANCHOR CATT SADLER QUIT ONCE SHE LEARNED THAT SHE WAS MAKING FAR

LESS THAN A MALE COHOST AND DURING THE CEREMONY NATALIE PORTMAN TOOK A BLUNT

AND SATISFYING DIG AT THE ALLMALE ROSTER OF NOMINATED DIRECTORS HOW COULD

THAT BE TOPPED

AS IT TURNS OUT AT LEAST IN TERMS OF THE OSCARS IT PROBABLY WONT BE

WOMEN INVOLVED IN TIMES UP SAID THAT ALTHOUGH THE GLOBES SIGNIFIED THE

INITIATIVES LAUNCH THEY NEVER INTENDED IT TO BE JUST AN AWARDS SEASON

CAMPAIGN OR ONE THAT BECAME ASSOCIATED ONLY WITH REDCARPET ACTIONS INSTEAD

A SPOKESWOMAN SAID THE GROUP IS WORKING BEHIND CLOSED DOORS AND HAS SINCE

AMASSED MILLION FOR ITS LEGAL DEFENSE FUND WHICH AFTER THE GLOBES WAS

FLOODED WITH THOUSANDS OF DONATIONS OF OR LESS FROM PEOPLE IN SOME

COUNTRIES

NO CALL TO WEAR BLACK GOWNS WENT OUT IN ADVANCE OF THE OSCARS THOUGH THE

MOVEMENT WILL ALMOST CERTAINLY BE REFERENCED BEFORE AND DURING THE CEREMONY

ESPECIALLY SINCE VOCAL METOO SUPPORTERS LIKE ASHLEY JUDD LAURA DERN AND

NICOLE KIDMAN ARE SCHEDULED PRESENTERS

ANOTHER FEATURE OF THIS SEASON NO ONE REALLY KNOWS WHO IS GOING TO WIN BEST

PICTURE ARGUABLY THIS HAPPENS A LOT OF THE TIME INARGUABLY THE NAILBITER

NARRATIVE ONLY SERVES THE AWARDS HYPE MACHINE BUT OFTEN THE PEOPLE FORECASTING

THE RACE SOCALLED OSCAROLOGISTS CAN MAKE ONLY EDUCATED GUESSES

THE WAY THE ACADEMY TABULATES THE BIG WINNER DOESNT HELP IN EVERY OTHER

CATEGORY THE NOMINEE WITH THE MOST VOTES WINS BUT IN THE BEST PICTURE

CATEGORY VOTERS ARE ASKED TO LIST THEIR TOP MOVIES IN PREFERENTIAL ORDER IF A

MOVIE GETS MORE THAN PERCENT OF THE FIRSTPLACE VOTES IT WINS WHEN NO

MOVIE MANAGES THAT THE ONE WITH THE FEWEST FIRSTPLACE VOTES IS ELIMINATED AND

ITS VOTES ARE REDISTRIBUTED TO THE MOVIES THAT GARNERED THE ELIMINATED BALLOTS

SECONDPLACE VOTES AND THIS CONTINUES UNTIL A WINNER EMERGES

IT IS ALL TERRIBLY CONFUSING BUT APPARENTLY THE CONSENSUS FAVORITE COMES OUT

AHEAD IN THE END THIS MEANS THAT ENDOFSEASON AWARDS CHATTER INVARIABLY

INVOLVES TORTURED SPECULATION ABOUT WHICH FILM WOULD MOST LIKELY BE VOTERS

SECOND OR THIRD FAVORITE AND THEN EQUALLY TORTURED CONCLUSIONS ABOUT WHICH

FILM MIGHT PREVAIL

IN IT WAS A TOSSUP BETWEEN BOYHOOD AND THE EVENTUAL WINNER BIRDMAN

IN WITH LOTS OF EXPERTS BETTING ON THE REVENANT OR THE BIG SHORT THE

PRICE WENT TO SPOTLIGHT LAST YEAR NEARLY ALL THE FORECASTERS DECLARED LA

LA LAND THE PRESUMPTIVE WINNER AND FOR TWO AND A HALF MINUTES THEY WERE

CORRECT BEFORE AN ENVELOPE SNAFU WAS REVEALED AND THE RIGHTFUL WINNER

MOONLIGHT WAS CROWNED

THIS YEAR AWARDS WATCHERS ARE UNEQUALLY DIVIDED BETWEEN THREE BILLBOARDS

OUTSIDE EBBING MISSOURI THE FAVORITE AND THE SHAPE OF WATER WHICH IS

THE BAGGERS PREDICTION WITH A FEW FORECASTING A HAIL MARY WIN FOR GET OUT

BUT ALL OF THOSE FILMS HAVE HISTORICAL OSCARVOTING PATTERNS AGAINST THEM THE

SHAPE OF WATER HAS NOMINATIONS MORE THAN ANY OTHER FILM AND WAS ALSO

NAMED THE YEARS BEST BY THE PRODUCERS AND DIRECTORS GUILDS YET IT WAS NOT

NOMINATED FOR A SCREEN ACTORS GUILD AWARD FOR BEST ENSEMBLE AND NO FILM HAS

WON BEST PICTURE WITHOUT PREVIOUSLY LANDING AT LEAST THE ACTORS NOMINATION

SINCE BRAVEHEART IN THIS YEAR THE BEST ENSEMBLE SAG ENDED UP GOING TO

THREE BILLBOARDS WHICH IS SIGNIFICANT BECAUSE ACTORS MAKE UP THE ACADEMYS

LARGEST BRANCH THAT FILM WHILE DIVISIVE ALSO WON THE BEST DRAMA GOLDEN GLOBE

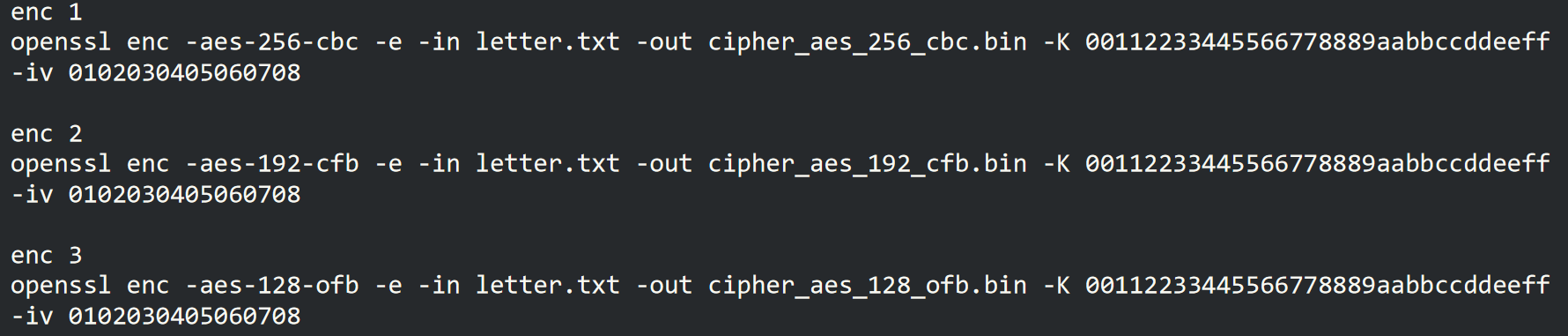
AND THE BAFTA BUT ITS FILMMAKER MARTIN MCDONAGH WAS NOT NOMINATED FOR BEST

DIRECTOR AND APART FROM ARGO MOVIES THAT LAND BEST PICTURE WITHOUT ALSO

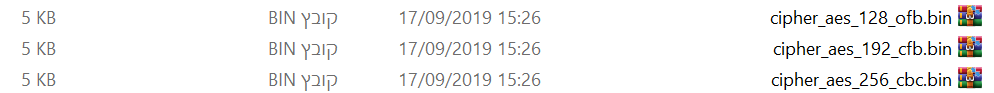
EARNING BEST DIRECTOR NOMINATIONS ARE FEW AND FAR BETWEEN

# Task 2

I used these commands-



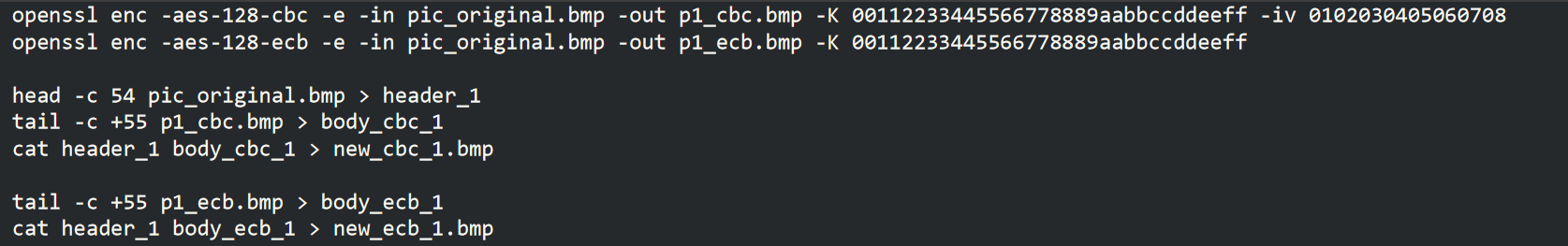
And got these files-



# Task 3

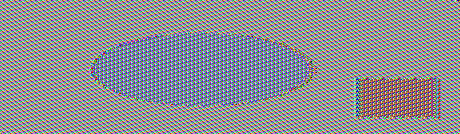
## Question 1

The commands we used for question 1 are-



## Question 2

ECB picture after encrypting-



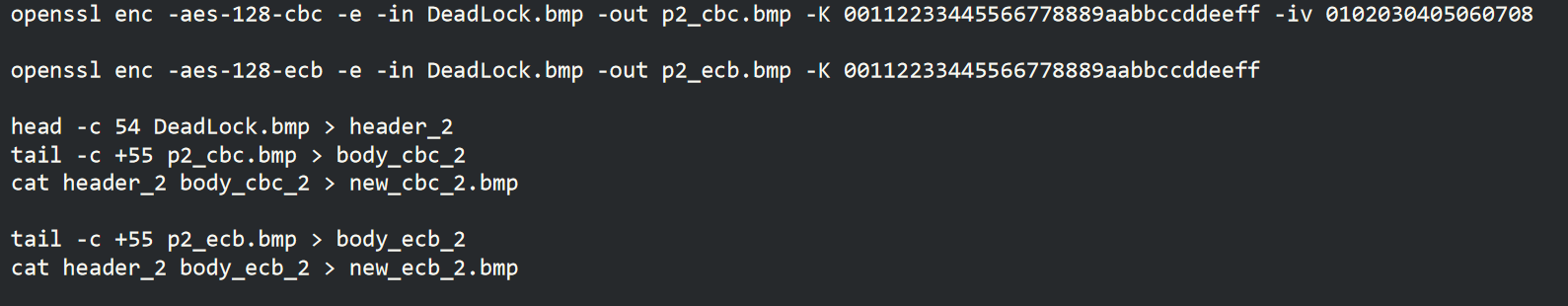
CBC picture after encrypting - g-

We can see that because ecb only encrypts each block with a certain key, we can still understand the general shapes of the picture. Unlike CBC, in which the blocks are codependent.

The picture I’ve selected is this:



And the this is the code I used -



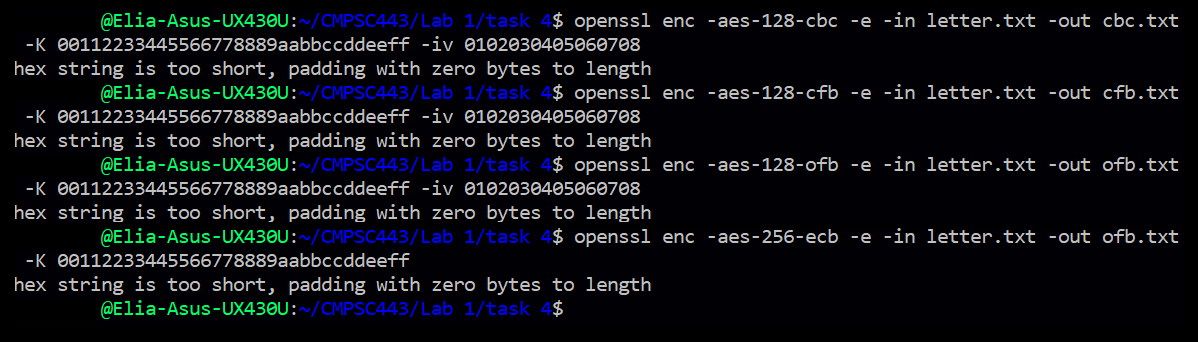
But for some reason I could not open the file after I repeated the process.  
I think it happened because I used a picture which was jpeg format, and changed it’s format to bmp and then did the process on it.

# Task 4

## Question 1

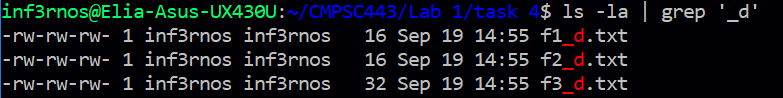
In my try, the results show that ECB, CBC, CFB, and OFB request padding.

but we can see that CFB, OFB modes does not need padding, because those modes are doing:  
plaintext XOR block cipher’s output  
while CBC and ECB modes are inserting the plaintext into the block cipher and therefore require a fixed size for the inserted plaintext

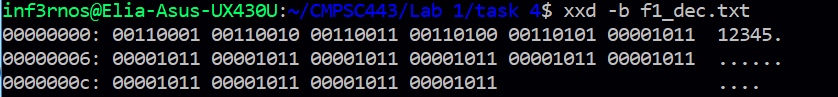


## Question 2

Sizes of the encrypted files (f1 : 5 bytes, f2 : 10 bytes, f3 : 16 bytes)

The padding is bytes of - 00001011 (binary) / 0b (hexadecimal)



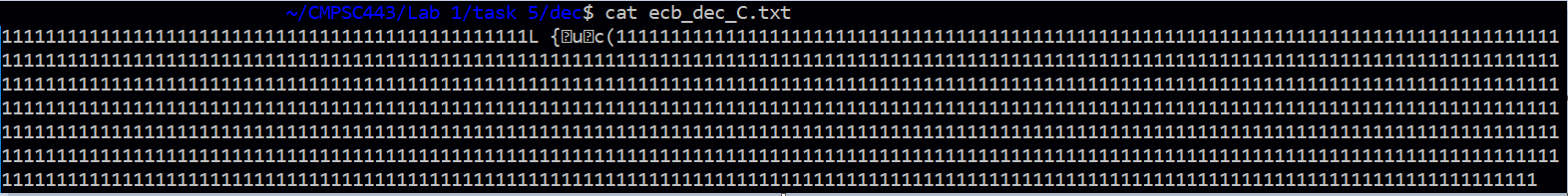
# Task 5

## Before the task

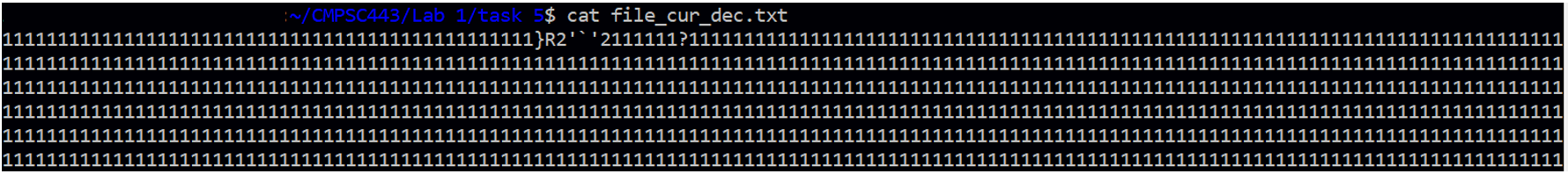
I assume that in ECB only the current block will be damaged, because each block is independent from the other blocks and does not affect their encryption and decryption.

CBC, the block and the one after him will be damaged, because the damaged cipher text is used to xor the next block when it exits the algorithm.  
  
in CFB the next block will be damaged, and the current block will be damaged in 1 byte.  
Because we use the ciphertext to xor the result of the algorithm in the current block, but we use the block as a input for the algorithm of the next block.  
  
in OFB the damage will be minimal because the ciphertext is only xor-ed with the result of the algorithm in his block, and is not inserted to another algorithm, so probably only a byte will be damaged (the 55th one).

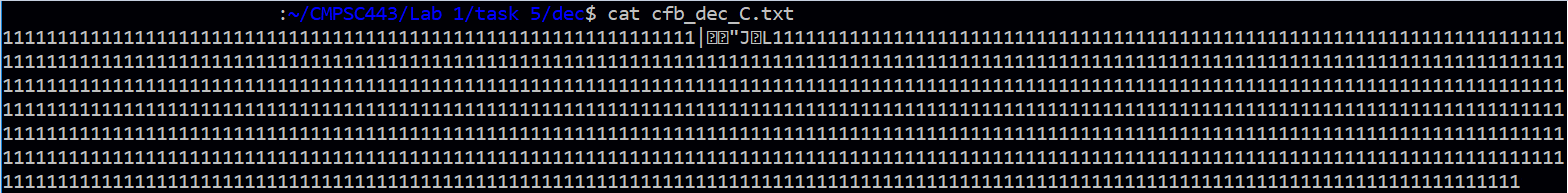
ECB



We can see that in ECB only the corrupted block is damaged, because each block is independent from the other blocks and does not effect them

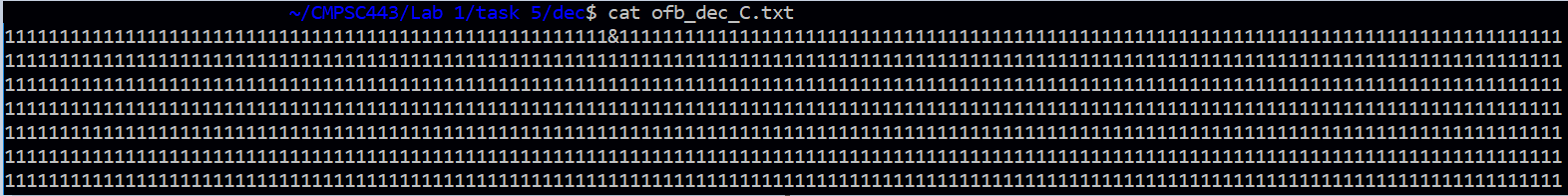
CBC  
we can see the one block got corrupted and we can see a question mark in the block after him.  
because in CBC we use the cipher text of the previous block to xor the result of the current block, the corrupted block effected the block after him.

CFB



We can see that only that only the next block was damaged, unlike what we assumed that the current block will also have a damaged byte.

OFB



As we assumed, only one byte is damaged.

# Task 7

The idea was to read the words from the given text (taking out the ‘\n’), using that word as a key for the encryption function, which we copied from the URL.  
and then comparing between the given ciphertext and the ciphertext our function generated.  
if they match, we can stop, because we have found the correct key.  
I had problems with changing the IV input, so I have changed it online and inserted it to the code.  
and another important thing was to close the files when we are finished with them.

## The Code

#include <openssl/evp.h>

#include <stdio.h>

#include <stdlib.h>

#include <stdbool.h>

#include <string.h>

#define CLOSE\_FILES fclose(plain);fclose(words);fclose(out);

void strcpy2(unsigned char dest[], char\* src){

int i = 0;

while(src[i] != '\0' && src[i] != '\n'){

dest[i] = src[i];

i++;

}

dest[i] = '\0';

}

int do\_crypt(FILE\* in, FILE\* out, int do\_encrypt, unsigned char iv[], unsigned char key[]);

void get\_new\_key(FILE\* words, unsigned char key[17]){

size\_t len = 0;

char\* line = 0;

getline(&line, &len, words);

strcpy2(key, line);

if (strlen(key)<17){

int i = strlen(key);

while(i<16) key[i++] = '#';

key[16]='\0';

}

}

int main(){

unsigned char iv\_aux[] = "226943873990930483007034637375096693265";

unsigned char\* iv = iv\_aux;

//dont with IV

unsigned char ciphertext[] = "062ff0112cb32d04d0adcfa02d215abd40a5f932da1ebbd3744de5d16be5a4d7";

unsigned char key[17];

unsigned char cipher\_for\_check[64];

//opening files

FILE\* plain = fopen("../file", "r");

if(plain == NULL) return -1;

FILE\* words = fopen("../words.txt", "r");

if(words == NULL){

fclose(plain);

return -1;

}

FILE\* out = fopen("../out", "w");

if(out == NULL){

fclose(plain);

fclose(words);

return -1;

}

//done with files

//try the keys

bool not\_found = true;

while(not\_found){

get\_new\_key(words, key);

do\_crypt(plain, out, 1, iv, key);

size\_t len = 0;

char\* line = 0;

getline(&line, &len, out);

strcpy2(cipher\_for\_check, line);

if(!(strcmp(cipher\_for\_check, ciphertext))){

printf("key is: %s\n", key);

not\_found = false;

}else{

fclose(plain);

plain = fopen("./file", "r");

}

}

CLOSE\_FILES

return 0;

}

int do\_crypt(FILE\* in, FILE\* out, int do\_encrypt, unsigned char iv[], unsigned char key[]){

// Allow enough space in output buffer for additional block

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

int inlen, outlen;

EVP\_CIPHER\_CTX\* ctx\_t = EVP\_CIPHER\_CTX\_new();

// Don't set key or IV right away; we want to check lengths

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

EVP\_CipherInit\_ex(ctx\_t, EVP\_aes\_128\_cbc(), NULL, NULL, NULL,

do\_encrypt);

OPENSSL\_assert(EVP\_CIPHER\_CTX\_key\_length(ctx\_t) == 16);

OPENSSL\_assert(EVP\_CIPHER\_CTX\_iv\_length(ctx\_t) == 16);

// Now we can set key and IV

EVP\_CipherInit\_ex(ctx\_t, NULL, NULL, key, iv, do\_encrypt);

for(;;){

inlen = fread(inbuf, 1, 1024, in);

if(inlen <= 0) break;

if(!EVP\_CipherUpdate(ctx\_t, outbuf, &outlen, inbuf, inlen)){

// Error

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

return 0;

}

fwrite(outbuf, 1, outlen, out);

}

if(!EVP\_CipherFinal\_ex(ctx\_t, outbuf, &outlen)){

// Error

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

return 0;

}

fwrite(outbuf, 1, outlen, out);

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

return 1;

}