

```
#include <stdio.h>
#include <string.h>
#include <stdlib.h>
#include <openssl/evp.h>

int main()
{
    int i,j;
    FILE *fp;
    int outlen, tmplen, inlen;

    unsigned char outbuf[65]; // RESULTING CIPHERTEXT
    unsigned char outbuf_hex[65]; // CONVERT ASCII CIPHERTEXT TO HEX CIPHERTEXT
    unsigned char key[16]; // KEY INITIALIZE
    unsigned char key_int[16]; // INT VERSION OF CHAR [] OF KEY

    EVP_CIPHER_CTX ctx;
    unsigned char iv[] = {0x01,0x02,0x03,0x04,0x05,0x06,0x07,0x08,0x09,0x0a,0x0b,0x0c,0x0d,0x0e,0x0f};
    unsigned char C[] = "32c956ba071e4fffbad37c2bb5b1a2e1585fbfcf649d88a9777b9ecd44639898";
    char intext[22] = "This is not a secret.";

    fp = fopen("words.txt", "r"); // READ WORDS TEXT FILE

    if (fp == NULL) // CHECK FILE
    {
        perror("Error while opening the file.\n");
        exit(EXIT_FAILURE);
    }

    while(fgets(key, sizeof key, fp)){ // LOOP THROUGH KEYS

        memset(outbuf_hex,0,sizeof(outbuf_hex)); // EMPTY OUT ARRAYS...
        memset(outbuf,0,sizeof(outbuf));
        memset(key_int,0,sizeof(key_int));

        key[strlen(key) - 1] = '#'; // CONVERT \N TO #

        for(i = 0; i < strlen(key); i++){ // LOOP THROUGH KEY CHAR []
            key_int[i] = (int)key[i]; // CONVERT ALL CHAR KEY TO INT
        }

        for(i = strlen(key); i < 16; i++){ // LOOP TO REMAINING KEY LENGHT (REACH 128)
            key_int[i] = 35; // APPEND # -> 0x23 -> 35 AS INT
        }

        EVP_CIPHER_CTX_init(&ctx); // INITIALIZE EVP CTX
        EVP_EncryptInit_ex(&ctx, EVP_aes_128_cbc(), NULL, key_int, iv); //PASS ARGUMENTS

        if(!EVP_CipherUpdate(&ctx, outbuf, &outlen, intext, strlen(intext))) //UPDATE OUTBUF WITH CIPHERTEXT
        {
            /* Error */
            printf("ERROR!");
            return 0;
        }

        if(!EVP_CipherFinal_ex(&ctx, outbuf + outlen, &tmplen)) // FINALIZE CIPHERTEXT
        {
            /* Error */
            return 0;
        }

        EVP_CIPHER_CTX_cleanup(&ctx); // CLEAR OUT EVP.CTX

        for(i = 0, j = 0; i < strlen(outbuf); i++,j+=2){ // LOOP THROUGH CIPHERTEXT
            sprintf((char*)outbuf_hex+j,"%02x",outbuf[i]); // CONVERT ASCII TO HEX W/O 0X..
        }

        if(!strcmp(outbuf_hex,C)){ // CHECK IF CIPHERTEXTS MATCH
            key[strlen(key) - 1] = 0;
            printf("KEY: %s\n",key); // PRINT KEY
            break; // EXIT OUT OF LOOP
        }
    }

    fclose(fp); // CLOSE WORDS.TXT
    return 0;
}
```