* Copied and pasted evp-symmetric-encrypt.c. from <https://wiki.openssl.org/index.php/EVP_Symmetric_Encryption_and_Decryption>
* Copied in our plaintext and iv
* Tested with that to see how it works
* In the “encrypt” method, changed EVP\_aes\_256\_cbc() to EVP\_aes\_128\_cbc()
* In the “decrypt” method, changed EVP\_aes\_256\_cbc() to EVP\_aes\_128\_cbc()
* Read in each word word by word
* Added the “#”s to each word to make it 16 characters if it was not already
* Put those words in as the key
* Entered BIO\_dump\_fp red herring
  + Saw there was hex in the text that it out put
  + Spent a lot of time trying to get the text into a text file that we could use
  + Read the text file containing the output from BIO\_dump\_fp
  + Got rid of the extra characters at the start and end
  + Got rid of the spaces and “-“
  + Compared that hex text with the given cipher text
  + Compared cipher texts
  + Didn’t get any matches
* Realized we should just use ciphertext instead of the BIO\_dump\_fp output
* Ciphertext just printed random garbage
* You sent out the email about how to change the binary output to hex
* We added that to our code and got just cipher texts, with no extra garbage
* Still no matches
* Realized we were entering the IV wrong
  + Put it in 0x format
* Found a match
* Printed the word that had been encrypted that had the matching ciphertext
* It was nature##########

A screenshot of a social media post

Description automatically generatedA screenshot of a social media post

Description automatically generatedA screenshot of a social media post

Description automatically generated

