Gotta Crack Them All

In this exercise we were given the task of acquiring the password of an admin in an nc connection. The nc connection provided the user with the ability to enter a phrase and submit it. If the phrase was already present it would present you with the encoded version, otherwise it would present nothing of use.

We were given three files:

- .txt file containing a list of leaked passwords (the admin password was among them)
- .txt file containing one of the passwords present in the nc connection
- .py file containing the algorithm used to encrypt the passwords.

To solve the CTF the following procedure was done:

1. The password given was submitted to the nc connection and it provided the following response b'kz\xc6\xb9\xd9Du\xcb\x8a\x9e\xe0\x9d\xbeo\xee\x03\xcf\xddd'
2. Looking at the .py file provided we noticed that the encryption used for the passwords in the service was a xor encryption. This meant that each byte of a password was performed a xor operation with a key. This key would be used to encrypt the password provided.
3. To decrypt all the passwords provided in the .txt file it was necessary to get the key that was previously mentioned.
4. To get the key we reversed the encryption function provided so that instead of giving us an encrypted password when a password was inputted it would give the key used for an encrypted password.
5. The new function (decrypt) performed a xor operation between an encrypted password and the unencrypted version of it.This in turn provided the key used for the encryption given that the xor operation is reversible.(A xor B = C,A xor C =B, B xor C = A).
6. Using the password given in the .txt file provided and its encrypted version we can get the key used for password encryption.
7. This key is not complete given that when it is used on the list of encrypted files it fails to completely decrypt a portion of them. This is because we found a portion of the key which corresponded to the length of the given password.
8. To get the entirety of the key step 6 is performed again but with one of the partially decrypted passwords and their fully encrypted version. This can be done for the reason that all passwords in the service are combinations of words, which means that if a password has only one character that was not decrypted then you can guess it based on context.
9. This process is repeated until the complete key is formed.
10. When the key is obtained it is possible to decrypt the admin's password.
11. With the admin's password decrypted we obtain the flag for the challenge.