Cada exercici **està explicat** al document **1. PRACTICA PHP - Encriptació Strings.pdf** del GitHub, també ho pots trobar al portfolio, a més dels fitxers php. Tot i així, en termes generals, l'explicació seria:

1. Crea la funció per desencriptar els diferents textos. *Recomenable fer una ullada a les funcions de tractament d'strings*

En aquesta activitat, faig un programa que:
· primer em talla en strings de 3 caracters i seguidament inverteix l'ordre (abc passa a ser cba)
· Després ajunto l'array amb implode per convertir-ho a string
· Amb un for-each, passo cada lletra al seu antònim comparant la seva posició a l'abecedari (si la c té la posició 3 al abecedari, per trobar el seu antònim faig posició de Z menys 3)
· Ajunto el resultat y retorno la string.

---

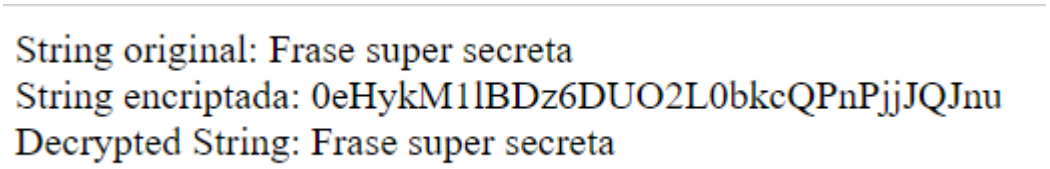
2. El sistema proposat per encriptar és poc segur i una mica rudimentàri. Busca una solució segura per encriptar i desencriptar text amb php. Explica breument com funciona, i mostra un exemple del seu funcionament.

En aquesta activitat, trobo una funció anomenada openssl_encrypt() i openssl_decrypt() que, a base de especificar paràmetres, em permet encriptar i desencriptar qualsevol text. La funció openssl_encrypt demana com a paràmetre el cifrat, i a partir d'aquest, fa un algorisme, en el meu cas, he escollit el cifrat AES CTR 128, el què fa es generar bits random amb la clau que li donem i l'IV (que és un número random que ens inventem), a partir d'aqui, es fa XOR amb la nostra string a encriptar, això crea un text randomitzat

Per desencriptar-ho, simplement hem de XOR el text amb els mateixos bits els quals hem generat a partir de la clau i l'IV

I què és XOR? XOR compara dos bits i en genera un com a resultat. La lògica a seguir és: si els bits són iguals, el bit resultant és 0, si els bits són diferents, el bit resultant és 1

L'exemple del seu funcionament seria:



3. Crea una técnica d'encriptament i desencriptament pròpia i original que compleixi els diferents requisits:

- Ha de funcionar per qualsevol caràcter UTF8.
- El text encriptat resultant contindrà només caràcters alfanumérics.
- El sistema d'encriptació ha de dependre de l'IP d'accés, de manera que amb una IP diferent no hauriem de ser capaços d'obtenir el text encriptat.

Explicacio de com funciona en termes generals:

ENCRIPTACIÓ:
Agafa la frase, una clau secreta i la ip, i el primer que fa és girar la string, tot seguit, barreja la string, ajunta l'ip, la string i la clau secreta, i un array de lletres i numeros random, i ho passa a base 64, i de base 64 a base 62. D'aquesta manera tenim l'alfanumèric encriptat.

DESENCRIPTACIÓ:
A partir d'introduir els paràmetres frase, clau secreta i ip, el primer que fa és convertir l'alfanumèric a string normal. Després reemplaça l'ip per espai buit i tot a partir de la clau secreta a buit, tot seguit, barreja la frase, i finalment gira la frase.

Accepta UTF-8, es pot introduir com a frase una ip i funcionarà igual, es pot introduir la clau secreta i es mantindrà, etc. No és un gran mètode però és efectiu.

Exemple sap la clau i la ip es igual:

Abans d'encriptar: Alex tot be?

després d'encriptar Ojox8JUnM3aisQmEFsIHRvdCB4ZWJlP0xpc3lhM2VkYWU5MTI2NjRhM2E1ZWIyMDQzNDI5

després de desencriptar Alex tot be?

Exemple no sap la clau i la ip es diferent:

Abans d'encriptar: Alex tot be?

després d'encriptar Ojox8JUnM3aisQmEFsIHRvdCB4ZWJlP0xpc3liZjNkNDI0NTQzMTE1MGI5MjZmZTNlNGV1

després de desencriptar ::1Al t29b0511345424d3fbysiL?ebex to6fe3e4ee