En un fitxer del servidor ens trobem amb el següent codi. Sabem que les dues cadenes de caràcters s'han encriptat mitjançant la següent codificació:

1. Es divideix el text amb cadenes de 3 caràcters. A cada tercet s'inverteix l'ordre dels caràcters, de manera que "abc" passa a ser "cba".
2. Remplecem els caràcters alfabètics per el seu oposat, de manera que 'a' passa a ser 'z', 'b' passa a ser 'y'... Els caràcters no alfabètics es mantenen.

Activitats

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

```php
function decrypt($string){
$abecedari = "abcdefghijklmnopqrstuvwxyz";
$stringSplitted = spliceAndInvert($string);
$stringSplitted = implode($stringSplitted);
$stringSplitted = str_split($stringSplitted);
foreach($stringSplitted as $index => $letter){

if(stripos($abecedari,$stringSplitted[$index])){
    $indexInitial = stripos($abecedari,$stringSplitted[$index]);
    $indexZ= stripos($abecedari,"Z");
    $stringSplitted[$index]=$abecedari[$indexZ-$indexInitial];
}
}
return implode($stringSplitted);
}

function spliceAndInvert($string){
$array = str_split($string, 3);
//Ara tens un array tal que Array[0]="hol" Array[1]="a b" etc
foreach($array as $clau => $valor){
$array[$clau] = strrev($valor);

}
return $array;

}
```

supercalifragilisticexpialidocious
es el alcalde el que quiere que sean los vecinos el alcalde. a veces lo mejor es no tomar decisiones, y eso en si, es una decision.

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.

```php
<?php
$simple_string = "Frase super secreta <br>";
echo "String original: " . $simple_string;
$ciphering = "AES-128-CTR";
$iv_length = openssl_cipher_iv_length($ciphering);
$encryption_iv = '1234567891011121';
$encryption_key = "Clausecreta";
$encryption = openssl_encrypt($simple_string, $ciphering,$encryption_key,
$options, $encryption_iv);
echo "String encriptada: " . $encryption . "<br>";
$decryption_iv = '1234567891011121';
$decryption_key = "Clausecreta";
$decryption=openssl_decrypt ($encryption, $ciphering, $decryption_key, $options,
$decryption_iv);

echo "Decrypted String: " . $decryption. "<br>";
?>
```

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

```
String original: Frase super secreta
String encriptada: 0eHykM1lBDz6DUO2L0bkcQPnPjjJQJnu
Decrypted String: Frase super secreta
```

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 ::1A1 t29b0511345424d3fbysiL?ebex to6fe3e4ee

EL CODI A LA SEGÜENT PÀGINA

```php
<?php

$string = "🐘Alex tot be?";
echo "<br>Abans d'encriptar: $string <br>";
$secretKey = "Lisy";
$ip = getIPAddress();

$stringEncriptada = encrypt($string, $secretKey, $ip);

echo "<br>després d'encriptar $stringEncriptada <br>";

//Per simular que no sap la clau i la ip es diferent:
/*
$secretKey = "wrongKey";
$ip ="126.333.111.50";
*/
//Per simular que sap la clau i la ip es igual:
/*
$secretKey = "Lisy";
$ip =getIPAddress();
*/

$stringDesencriptada = (decrypt($stringEncriptada, $secretKey, $ip));

echo "<br>després de desencriptar $stringDesencriptada <br>";

/**
 *
 * Encripta una string i la converteix a
 * alfanumeric (base 62)
 * @return string
 *
 */
function encrypt($string, $secretKey, $ip)
{

    $string = mb_strrev($string);
    $string = swapArray($string);
    $string = stringtoBase62($string, $secretKey, $ip);
    return $string;
}
/**
```

```
 *
 * A partir d'una string, te la decripta
 * @return string
 *
 */
function decrypt($string, $secretKey, $ip)
{

    $string = base62toString($string, $secretKey, $ip);
    $string = swapArray($string);
    $string = mb_strrev($string);

    return $string;
}

/**
 *
 * Passa string a alfanumeric, tot concatenant l'ip al principi i
secretKey al final
 * i un seguit de numeros i lletres random despres de la clau secreta
 *
 * @param  string $string String a convertir
 * @param  string $secretKey clau secreta per desencriptar
 * @param  string $ip ip del usuari
 * @return string
 *
 */
function stringtoBase62($string, $secretKey, $ip)
{
    $arrayLiante = [];
    for($i=0;$i<5;$i++){
        $rand = substr(md5(microtime()),rand(0,26),5);
        $arrayLiante[]=$rand;
    }

    $string = $ip . $string . $secretKey.implode($arrayLiante);
    $string = base64_encode($string);
    $string = base64to62($string);
    return $string;
}

/**
```

```
 *
 * Passa alfanumeric (base 62) a string
 *
 * @param  string $string String a convertir
 * @param  string $secretKey clau secreta per desencriptar
 * @param  string $ip ip del usuari
 * @return string
 *
 */
function base62toString($string, $secretKey, $ip)
{
$string = base62to64($string);
    $string = base64_decode($string);

    $string = preg_replace('/' . $ip . '/', "", $string, 1);
    /*
    Si la ip no la troba, no fara un replace, i per tant, depen de
l'ip per desencriptar
    el preg_replace em permet que nomes ho canvii un cop, per tant
poden posar 127.etc etc com a frase i es mante
    */
    $lastOcurrenceSK = strrpos($string, $secretKey);

    //Si la clau secreta no es bona, l'array liante d'abans fara que
sigui una frase molt rara
    if ($lastOcurrenceSK) {
        $string = substr($string, 0, $lastOcurrenceSK);
    }

    return $string;
}


/**
 *
 * Agafa una string i barreja la primera posicio amb la ultima,
segona amb penultima...
 *
 * @param  string $string String a barrejar
 * @return string
 *
 */
```

```php
function swapArray($string)
{

    $array = mb_str_split($string, 1, 'UTF-8');
    $arrayLength = count($array) - 1;
    for ($i = 0; $i <= $arrayLength / 6; $i++) {
        $aux = $array[$i];
        $array[$i] = $array[$arrayLength - $i];
        $array[$arrayLength - $i] = $aux;
    }

    return implode($array);
}

/**
 *
 * Gira una string UTF-8
 *
 * @param  string $string String a girar
 * @param  string $encoding codificacio de la string
 * @return string
 *
 */
function mb_strrev($string, $encoding = null)
{
    if ($encoding === null) {
        $encoding = mb_detect_encoding($string);
    }

    $length = mb_strlen($string, $encoding);
    $reversed = '';
    while ($length-- > 0) {
        $reversed .= mb_substr($string, $length, 1, $encoding);
    }

    return $reversed;
}

/**
 *
 * Aconsegueix l'ip de l'usuari
 * (funcio no segura, es pot bypass)
```

```php
 * @return string
 *
 */
function getIPAddress()
{
    //whether ip is from the share internet
    if (!empty($_SERVER['HTTP_CLIENT_IP'])) {
        $ip = $_SERVER['HTTP_CLIENT_IP'];
    }
    //whether ip is from the proxy
    elseif (!empty($_SERVER['HTTP_X_FORWARDED_FOR'])) {
        $ip = $_SERVER['HTTP_X_FORWARDED_FOR'];
    }
    //whether ip is from the remote address
    else {
        $ip = $_SERVER['REMOTE_ADDR'];
    }
    return $ip;
}

function base64to62($string)
{

    $array = str_split($string);

    for ($i = 0; $i < strlen($string); $i++) {
        $char = $array[$i];
        if ($char == "=") {
            $array[$i] = "UnUIG";
        } else if ($char == "/") {
            $array[$i] = "Una0Bar";
        } else if ($char == "+")
        $array[$i] = "UnM3ais";
    }

    return implode($array);
}

function base62to64($string)
{
$igual = "UnUIG";
$mes = "UnM3ais";
```

```
$barra = "Una0Bar";

    $string = preg_replace('/' . $igual . '/', "=", $string);
    $string = preg_replace('/' . $mes . '/', "+", $string);
    $string = preg_replace('/' . $barra . '/', "/", $string);

return ($string);

}
```