<?php

**require\_once**('vmscFunctions.php');

$ctext=**$\_GET**['asd'];

$n2h=**$\_GET**['n2h'];

$pk=**$\_GET**['pk'];

$userid=1;

$reply='<h4>Boo</h4><p>ctext<br>'.$ctext.'</p><p>dsa<br>'.$n2h.'</p>';

$query="select KeyPk,KeySk,Nonce

from cryptokeys

where UserId=?

and KeyTime=(select max(KeyTime) from cryptokeys where UserId=?)";

$types="ii";

$params=**array**($userid,$userid);

$result=*query*($types,$params,$query);

**while**($row=$result->fetch\_assoc()){

$keypk=$row['KeyPk'];

$keysk=$row['KeySk'];

$nonce=$row['Nonce'];

}*mysqli\_free\_result*($result);

$jsnonce=*sodium\_hex2bin*($n2h);

$keydc=$keysk.$pk;

$text=*sodium\_crypto\_box\_open*($ctext,$jsnonce,$keydc);

$reply.='<br>'.*strlen*($nonce).'<br>';

$reply.='<br>'.*strlen*($jsnonce).'<br>';

$reply.='<br>'.*strlen*($n2h).'<br>';

$reply.='<br>'.*sodium\_bin2hex*($keypk).'<br>'.*sodium\_bin2hex*($keysk).'<br>'.*sodium\_bin2hex*($nonce);

**echo**($reply);

?>