<?php

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

// echo(implode("<Br>",get\_loaded\_extensions()));

/\* echo(SODIUM\_LIBRARY\_VERSION );

 var\_dump([

 SODIUM\_LIBRARY\_MAJOR\_VERSION,

 SODIUM\_LIBRARY\_MINOR\_VERSION,

 SODIUM\_LIBRARY\_VERSION

 ]);

 $secret\_key = sodium\_crypto\_secretbox\_keygen();

 $message = 'Sensitive information';

 $nonce = random\_bytes(SODIUM\_CRYPTO\_SECRETBOX\_NONCEBYTES);

 $encrypted\_message = sodium\_crypto\_secretbox($message, $nonce, $secret\_key);

 $decrypted\_message = sodium\_crypto\_secretbox\_open($encrypted\_message, $nonce, $secret\_key);

 echo('<br>'.$secret\_key);

 echo('<br>'.$encrypted\_message);

 echo('<br>'.$decrypted\_message);

//Symmetric Encryption

echo('<br><br>Symmetric Encryption');

 $msg="This is a message";

 $key=random\_bytes(SODIUM\_CRYPTO\_SECRETBOX\_KEYBYTES);//32

 $nonce=random\_bytes(SODIUM\_CRYPTO\_SECRETBOX\_NONCEBYTES);//24

 $ciphertext=sodium\_crypto\_secretbox($msg,$nonce,$key);

 $plaintext=sodium\_crypto\_secretbox\_open($ciphertext,$nonce,$key);

 echo('<br>');

 echo($plaintext);

//Symmetric Authentication

echo('<br><br>Symmetric Authentication');

$msg="Another message";

$key=random\_bytes(SODIUM\_CRYPTO\_SECRETBOX\_KEYBYTES);

$mac=sodium\_crypto\_auth($msg,$key);

echo('<br>');

echo(sodium\_crypto\_auth\_verify($mac,$msg,$key)?"Yes":"No");

\*/

 //Public Key Encryption

 **echo**('<br>Public Key Encryption');

 $aliceKeypair=*sodium\_crypto\_box\_keypair*();

 $alicePublicKey=*sodium\_crypto\_box\_publickey*($aliceKeypair);

 $aliceSecretKey=*sodium\_crypto\_box\_secretkey*($aliceKeypair);

 $bobKeypair=*sodium\_crypto\_box\_keypair*();

 $bobPublicKey=*sodium\_crypto\_box\_publickey*($bobKeypair);

 $bobSecretKey=*sodium\_crypto\_box\_secretkey*($bobKeypair);

 **echo**('<br>'.*sodium\_bin2hex*($bobPublicKey));

 $msg='This is a secret message';

 $nonce=*random\_bytes*(*SODIUM\_CRYPTO\_BOX\_NONCEBYTES*);

 $keyEncrypt=$aliceSecretKey.$bobPublicKey;

 $cipherText=*sodium\_crypto\_box*($msg,$nonce,$keyEncrypt);

 //echo('<br>'.$cipherText);

 $keyDecrypt=$bobSecretKey.$alicePublicKey;

 $plaintext=*sodium\_crypto\_box\_open*($cipherText,$nonce,$keyDecrypt);

 **echo**('<br>');

 //echo($plaintext===$msg?'<br>Yes<br>':'<br>No?<br>');

 $test=*sodium\_bin2hex*(*sodium\_crypto\_box\_publickey*(*sodium\_crypto\_box\_keypair*()));

 $userid=1;

 $query='insert into cryptokeys(KeyId,KeyTime,KeyPk,KeySk,Nonce,UserId)values(null,now(),?,?,?,?)';

 $types="sssi";

 $params=**array**($bobPublicKey,$bobSecretKey,$nonce,$userid);

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

 $bobPublicKey=*sodium\_bin2hex*($bobPublicKey);

?>

<!DOCTYPE type="html">

<html lang=*"US"*>

<head>

 <link rel=*"shortcut icon"* href=*"include/icons/logo.png"* />

 <link rel=*"stylesheet"* href=*"vmsstyle.css"*>

 <title>test</title>

 <script src=*"lib/nacl\_factory.js"*></script>

</head>

<body>

 <h4>Sodium Javascript</h4>

 <button type=*"button"* onclick="ajax();">Do it</button>

 <div id=*"response"*>

 </div>

 <script type=*"text/javascript"*>

 **function** ajax(){

 **var** xhttp;

 **var** response;

 **var** akeypair;

 **if**(window.XMLHttpRequest){

 xhttp=**new** XMLHttpRequest();

 }**else**{

 xhttp=**new** ActiveXObject("Microsoft.XMLHTTP");

 }

 xhttp.onreadystatechange=**function**(){

 **if**(**this**.readyState==4 && **this**.status==200){

 document.getElementById("response").innerHTML=**this**.responseText;

 }

 };

 **var** bpkeypair;

 **var** msg='My message';

 **var** nonce='';

 **var** message='';

 **var** ctext;

 nacl\_factory.instantiate(**function**(nacl1){

 bpkeypair=nacl1.from\_hex("<?php **echo**($bobPublicKey); ?>");

 });

 alert("bpkeypair"+bpkeypair);

 nacl\_factory.instantiate(**function**(nacl){

 akeypair=nacl.crypto\_box\_keypair();

 message=nacl.encode\_utf8(msg);

 nonce=nacl.crypto\_box\_random\_nonce();

 // ctext=nacl.crypto\_box(nacl.encode\_utf8(msg),nacl.crypto\_box\_random\_nonce(),bpkeypair,nacl.crypto\_box\_keypair().boxSk);

 });

 alert('akeypair.boxPk'+akeypair.boxPk);

 alert('message'+message);

 alert('nonce'+nonce);

 **var** n2h='';

 nacl\_factory.instantiate(**function**(acl){

 ctext=acl.crypto\_box(message,nonce,bpkeypair,akeypair.boxSk);

 n2h=acl.to\_hex(nonce);

 });

 alert("ctext"+ctext);

 alert("n2h"+n2h);

 alert("akeypair"+akeypair.boxPk);

 xhttp.open("GET","\_\_testrespoonse.php?asd="+ctext+"&n2h="+n2h+"&pk="+akeypair.boxPk,**true**);

 xhttp.send();

 }

 </script>

</body>

</html>