

Forum:[Hack Forums](#)

Thread: [Help me convert this PHP code to C#](#)

draxyee - March 20, 2020, 8:04 am

PHP Code

```
<?php
```

```
$key = openssl_random_pseudo_bytes(32);  
$iv = openssl_random_pseudo_bytes(12);  
$time = time();
```

```
openssl_public_encrypt($key, $encryptedAesKey, base64_decode($publicKey));  
$encrypted = openssl_encrypt($password, 'aes-256-gcm', $key, OPENSSL_RAW_DATA, $iv,  
$tag, strval($time));
```

This is what I currently have:

Code

```
byte[] key = new byte[32];  
byte[] iv = new byte[12];  
RNGCryptoServiceProvider rng = new RNGCryptoServiceProvider();  
rng.GetBytes(key);  
rng.GetBytes(iv);  
string rngString = Encoding.UTF8.GetString(key);
```

```
string keyString =  
"LS0tLS1CRUdJTiBQVUJMSUMgS0VZLS0tLS0KTUIJQklqQU5CZ2txaGtpRzl3MEJBUUVGQUFPQ  
0FROEFNSUICQ2dLQ0FRRUF4ZmFic2RVSDJLenRJaGs5MG42eQpUdk9teGZZRWU5MXA3OW  
RKYkxwa2g0eXJnNmtCQVppeUVoUHNINIFpcHVxM2h0c0ppZnpGMzdIVUF0ODE2M3QxCnNLZXI  
BQzlxU0NKcndaUGZRb3ZyUHdlYjU1bVc2SGdZbUxsU0ovK2xKbzdsLzNzekRaYnd1dHVBYWxsZ  
U9oZUcKQnlrYVgrRFhQbDRwbWVYLzZDUHRYs1Bkdi9xUGRYRytOZS9JaHJCNEtKdzl4NElMbGt  
nR3ZjaS8wbIFKRjl1awpOYytVK3F2eE9TaWV4MjI2pIUnNWOGpadnNxoGh5Q1EyK2hwNmdkSE  
dxUGoveW1zRG14RHd4MUF1ZUIrVIZiCnlzQ0RjYzdHdTNDdpZXN6NTRXTXICQUFnVm9  
DSWRQMfU1Tis0S1duMWNhc1RoL3NZWVFFSFRaUis3UzcKcFFJREFRQUICKLS0tLS1FTkQgUF  
VCTEIDIEtFWS0tLS0tCg==";  
byte[] keyBytes = Convert.FromBase64String(keyString);  
string keyStringDecoded = Encoding.UTF8.GetString(keyBytes);
```

```
string timeString = ((int)(DateTime.UtcNow - new DateTime(1970, 1,  
1)).TotalSeconds).ToString();  
byte[] timeBytes = Encoding.UTF8.GetBytes(timeString);
```

```
OpenSSLProtect osp = new OpenSSLProtect();  
string encryptedAesKey = osp.OpenSSLEncrypt(rngString, keyStringDecoded);
```

```
EncryptionService iq = new EncryptionService(32, 16, 12);  
string encrypted = iq.EncryptWithKey(password, rngString, timeBytes);
```

I'm getting this error: "System.FormatException: 'The input is not a valid Base-64 string as it contains a non-base 64 character, more than two padding characters, or an illegal character among

the padding characters. ""

This is what I'm using for AES-256-GCM (EncryptionService / iq.EncryptWithKey):
<https://github.com/lukemerrett/Bouncy-Castle-AES-GCM-Encryption>

If anyone can help me, I would be so appreciative.

Cheers.