# Encrypt/Decrypt long string with PHP OpenSSL & key pairs

Have you ever tried to encrypt/decrypt long string (could be a JSON encoded string of an object?) with PHP OpenSSL and key pairs (private – public key)?
If yes, you could face the problem: returned value is NULL when your string is too long, is it a bug???


No, it's just a limitation of OpenSSL's algorithm 😕 So how we can do it?
Well, we can just use OpenSSL's encrypt method with key & IV, it allows long string encryption, but we will lose the profit of key pair. Because openssl_encrypt will encrypt with key & IV, but we don't want to share this key & IV (and that's why we want to use key pair encryption). And then it's probably not the solution which makes you happy.
Hey, but how's about we will use both (openssl_encrypt and openssl_private_encrypt)?
The idea is: We will create a key & IV (randomly? like current unix time plus random number), use them to encrypt the data. We also encrypt the key & IV with our private key. Then we share the encrypted data with encrypted key & IV. To decrypt data, your friend will need to use the public key to decrypt the key & IV, then use this key & IV to decrypt the encrypted data you sent.

Let’s go to the example:

- **Encryption**
- Create random key
- $password = sha1(microtime(true) . rand());
- Encrypt the key (given private key = key.private)
- openssl_private_encrypt($password, $passwordCrypted , file_get_contents("key.private"), OPENSSL_PKCS1_OAEP_PADDING);
- $passwordCrypted = base64_encode($passwordCrypted);
- Create IV, here I just make IV based on key, to simplify the process
- $iv = substr(md5($passwordCrypted), 0, 16);
- Finally, encrypt data with key (given $data = the(mixed) data you want to encrypt)
- $dataCrypted = openssl_encrypt(json_encode($data), 'aes128', $password, false, $iv);
- Now you can share the data to your friend:
- $passwordCrypted: Encrypted key
- $dataCrypted: Encrypted data

- **Decryption**
- Decrypt the key (given public key = key.pub)
- openssl_public_decrypt(base64_decode($passwordCrypted), $passwordDecrypted, file_get_contents("key.pub"));
- Get the IV
- $iv = substr(md5($passwordCrypted), 0, 16);
- Decrypt the data
- $dataDecrypted = json_decode(openssl_decrypt($dataCrypted, 'aes128', $passwordDecrypted, false, $iv, OPENSSL_PKCS1_OAEP_PADDING));