

AES-Crypt-PHP  
=====

Yet another PHP implementation of the open source aes crypt file format:  
.aes

Use the library to encrypt/decrypt files at your site with PHP. The files  
will be encrypted with 128-bit AES in CBC mode to a password of your choice.

Usage: Please see example.php

The project is a fork of IgoAtM:s code,  
originally published at:

<https://forums.packetizer.com/viewtopic.php?f=72&t=403>

The encrypted .aes files can be decrypted at almost any platform:

<https://www.aescrypt.com/>

<https://www.aescrypt.com/download/>

The file specification is described here:

[https://www.aescrypt.com/aes\\_file\\_format.html](https://www.aescrypt.com/aes_file_format.html)

This library supports version 2 of the file format.

Warning

-----

This library uses mcrypt;  
mcrypt doesn't encrypt text files correctly:

Windows line breaks are substituted by Linux line breaks.  
Thus the file doesn't hash the same after encryption-decryption,  
and pgp-signatures are invalid.

You could avoid the problem by compressing the file before encryption.