


[Show pagesource](#) [Old revisions](#)   [AdChoices](#) [AES 128 Bit](#) [AES Encrypt](#) [AES Key](#) [AES Code](#)

[Recent changes](#) [Search](#)

You are here: [Welcome to mbirth's Wiki](#) » [Code Snippets](#) » [JavaScript](#) » [AES / Rijndael](#)

AES / Rijndael

Table of Contents

- AES / Rijndael
 - Usage
 - See Also

Chris Veness has written a [JavaScript implementation](#) of AES in counter operation mode some time ago. I wrapped the code up into a class for easier use.

Download it here: [aes.class.js](#) (18.25 KiB, [933 downloads](#))

Usage

```
var text = 'Hello, world!';
var password = 'itsmysecret';
var blocksize = 256; // can be 128, 192 or 256

var crypted = AES.encrypt( text, password, blocksize );
// do something...
var decrypted = AES.decrypt( crypted, password, blocksize );
```

See Also

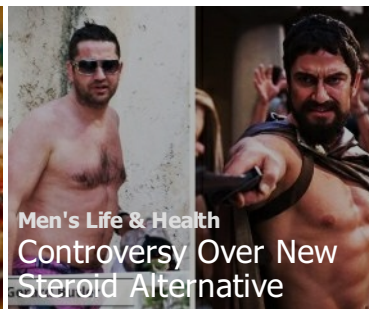
- [AES / Rijndael](#) — [PHP implementation](#) of this algorithm
- [AES / Rijndael](#) — [Python implementation](#) of this algorithm

Welcome to mbirth's Wiki

- Willkommen auf mbirth's Wiki
- Know-How
- Code Snippets
 - apache
 - AutoHotkey
 - C #
 - CMD/BAT
 - CSS
 - Excel
 - Java
 - JavaScript
 - AES / Rijndael**
 - Debugging
 - Get floating position
 - Unpack PACKED scripts
 - PHP
 - Python
 - SH
 - VBA
 - Software

Other pages

- [Homepage](#)



2 Comments mbirth's Wiki

Sort by Newest ▾

• 4 years ago

digi7al64

On line 187 you need to update the code to include the reference to 'this'

Original

```
var key = this.Cipher(pwBytes, KeyExpansion(pwBytes)); // gives us 16-byte key
```

Modified

```
var key = this.Cipher(pwBytes, this.KeyExpansion(pwBytes)); // gives us 16-byte key
```

↑
↓

• Reply • Share >

• 4 years ago

Markus Birth Mod

Thanks, I fixed it. :)

↑
↓

• Reply • Share >

Subscribe
 Add Disqus to your site

snippets/javascript/aes-rjndael.bt · Last modified: 2013-03-16 17:27:02 (external edit)

Show pagesource

Old revisions

Media Manager

Login

Sitemap

Back to top

Except where otherwise noted, content on this wiki is licensed under the following license: CC Attribution-Noncommercial-Share Alike 3.0 Unported

- Piwik
- SiteBar Bookmarks



THINKING OF
MIGRATING TO
ETHERNET?

**CALCULATE
YOUR COST
SAVINGS**

FIVE MINUTES IS
ALL IT TAKES!

GET STARTED

