



链滴

OpenSSL 和 Java AES 算法的的问题

作者: [turbidsoul](#)

原文链接: <https://ld246.com/article/1364029338305>

来源网站: [链滴](#)

许可协议: [署名-相同方式共享 4.0 国际 \(CC BY-SA 4.0\)](#)

<p> 开篇第一句话我想说，OpenSSL不支持与Java的对接，这是多么蛋疼的一话，不过确实是这样，原因是在c中的填充方式和Java中的填充方式不一样，Java不支持c中的/0的填充方式。</p>

<p> 具体信息请查看：<u>penSSL和JAVA AES算法的问题总结</u></p>

<p> 至于我为什么会写这篇文章呢，是我们的项目中有部分在网络传输的内容需要加密，所以就选了AES的，服务端使用的是openresty 这是淘宝的一个大写的，他里面集成了LuaJit，加密的部分使用的是resty.aes，而resty使用的是OpenSSL的C代码实现的加密解密。为了和OpenSSL实现对接，我就蛋疼的去简单的链接了下OpenSSL，在上面的文章中指导OpenSSL并不支持Java，查了无数人的文章，很多人都对这个问题很苦恼，最后在 stackoverflow 里找到了一个大牛给出了一个解码的实现 stackoverflow 我据这位大牛的代码简单的修改了一下，就做成了我需要的代码：OpenSSL.java</p>

<p>
 最后我想吐槽一下lua5.1居然不支持位运算，要5.2才支持，好吧，openresty集成的就5.1所以我在实现lua的16位编码解码果然蛋疼了一下。</p>