# 搜狐精准广告平台 AdExchange
# 成交价解密算法

## 1. 算法概述

采用 AES(Rijndael)密码对获胜价格进行加密。Rijndael 是使用对称密钥加解密的块加密密码体制，可以支持的加密块长度为 16Bytes 和 32Bytes，密钥长度可以为 16Bytes,24Bytes 和 32Bytes。在我们的应用中，选用的密钥长度为 32Bytes，密文块大小为 16Bytes。Rijndael 密码是基于伽罗瓦域 GF(28)上的多项式运算所设计的，其详细资料可参见附录一。附录二是采用本算法的三个测试用例。附件是使用 32Bytes 密钥对 16Bytes 大小的密文块进行脱密的 C 程序。

## 2. 密码协议

加密：我们首先将获胜价格转化为字符串，若字符串的长度不是 16Bytes 的整数倍，我们将在字符串后面补随机字符，直至字符串长度为 16Bytes 的整数倍。我们再在该字符串的末尾追加一个 16Bytes 的块，存放明文的真实长度。再使用 Rijndael 算法对整个字符串按 16Bytes 块大小进行加密。最后把密文转化为十六进制可见字符，显示在展示监测宏的 winprice 参数中。

解密：DSP 商首先将十六进制可见字符串转换为密文，然后依次对该密文的 16Bytes 块进行块解密。解密之后获取最后一个块的信息，得到明文的长度，即可获得实际的明文。

## 3. 举例说明

(1)加密：需要加密的信息为 win_price=3.14，生成待加密字符串，如图 1：

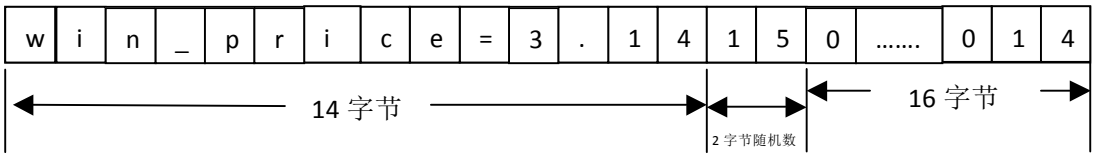


图 1

(2)上述信息为 32Bytes，加密后，将密文转换为 16 进制可见字符，转换后的长度为 64Bytes

(3)脱密：先将 64Bytes 字符串转换为 32Bytes 密文，脱密之后得到如图 1 所示的字符串。取后 16 字节，得到明文长度为 14，因此明文为 win_price=3.14。

# 附录一：参考文献：

http://csrc.nist.gov/archive/aes/rijndael/Rijndael-ammended.pdf

# 附录二：测试用例：

示例 1

明文：Hello World

十六进制密钥：

6F46756B794C5535777A3534494150326F72503155325177644E447267494843

十六进制密文：

2A0956BB2CF0AE98A10F0CA0DFDF396E51FF819D039C338A6F8185AB9209D9BF

示例 2

明文：5.5

十六进制密钥：

70465A507A31376F564E70344745303336625A30696B56794F7536316B565848

十六进制密文：

1CC76C4E999E87CFC06EB425D1672C591F28C4C9659C510A24B9BC147A37FB1A

示例 3

明文：www.sohu.com

十六进制密钥：

574A435543677446484A4F4C624263617063585A4D536E557A55516D4A675746

十六进制密文：

447DD39BEB3604ACB521D48DEDE870A01577DFC8D293DCC1B351EC72617E54AF